KPMG

FINSEC Law Advisors

The insider threat - Safeguarding UPSI from within: A refresh

January 2025

KPMG. Make the Difference.

Table of contents

SEBI regulations on the leakage of price sensitive information

The Securities and Exchange Board of India (SEBI) was among the first, and has been at the forefront in terms of delivering on a mandate that includes:

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

A key area of such regulatory governance has been with respect to preventing and penalising violations pertaining to insider trading. While the laws regarding insider trading were introduced in 1992, overtime it was felt that the regulations needed to be strengthened to serve the intended purpose.

Resultantly, the SEBI (Prohibition of Insider Trading) Regulations, 2015 ("PIT Regulations") were introduced. Further, the SEBI (Prohibition of Insider Trading (Amendment) Regulations, 2018 and the SEBI (Prohibition of Insider Trading (Amendment) Regulations, 2019 were notified. The amended regulations are aimed at ensuring accountability and a robust control framework to prevent insider trading.

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 phenomenon, known as 'Heard on Street' (HOS), is seen as a regular behaviour by brokers/analysts, however, recent events indicate that this conduct is questionable.

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(PIT), 2015[1] to combat the menace of trading in securities with the unfair advantage of having access to 'Unpublished price sensitive information' (UPSI), which when published, is likely to materially impact the price of securities in the market.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

Further, as per a 2024 amendment, SEBI clarified that unverified events or information reported in print or electronic media would not be considered as 'generally available information', and therefore, such information would be considered as UPSI if it is likely to materially impact the price of shares.

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 the PIT Regulations, read with section 12A (e) of the Securities and Exchange Board of India Act, 1992 (SEBI Act) which prohibits the procurement or communication of UPSI. The said provisions are read as under:

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

SEBI regulations on the leakage of price sensitive information

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 the 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 a fine, which may extend to INR25 crore or with both.

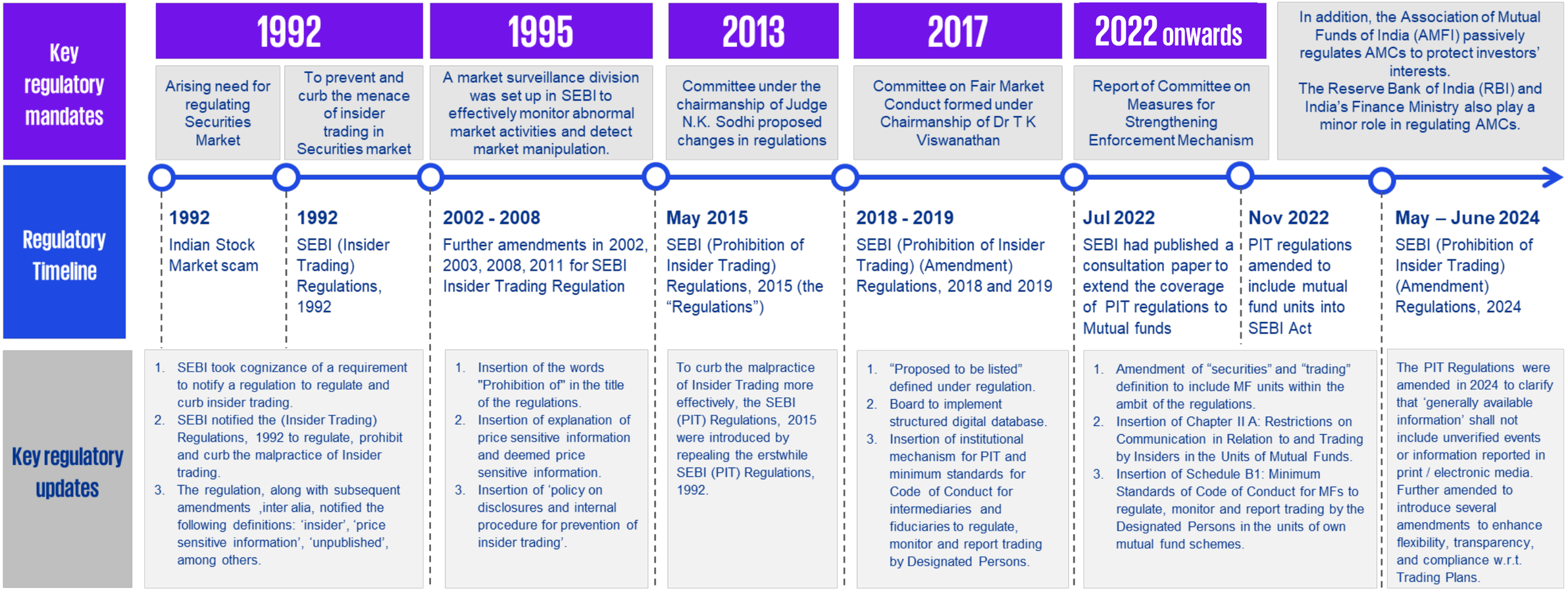
Complementing these regulations are the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 (LODR). LODR mandates that listed companies disclose material information promptly and transparently, ensuring that all stakeholders have equal access to critical information. This includes periodic financial results, shareholding patterns, and significant corporate actions. The LODR regulations are designed to enhance corporate governance standards and ensure that companies adhere to fair disclosure practices, thus protecting investor interests and promoting market integrity.

Additionally, the Companies Act, 2013, also plays a crucial role in regulating insider trading. It includes provisions under Section 195 (prohibition on insider trading of securities), which makes it illegal for any person, including company directors or officers, to deal in securities based on non-public, price-sensitive information. The Act also emphasises corporate governance and accountability, requiring companies to follow stringent disclosure norms and ethical practices.

3. THE SECURITIES LAWS (AMENDMENT) ACT, 2014, SEBI, 22nd August 2014, accessed on 1 March 2018

Amendments by SEBI

The following section provides an overview of the regulatory updates and various amendments to the PIT regulations since its inception. These changes aim to enhance transparency, ensure market integrity, and adapt to evolving market dynamics. Detailed explanations of these amendments and their implications are presented below:



Enforcement trends

SEBI is cracking down on insider trading with its stringent norms. Increased surveillance has brought higher number of instances of such violations to surface. In view of this, it has become even more imperative to sensitise companies and their employees regarding SEBI(PIT) Regulations, 2015, and amendments thereof.

₹74.88 Crore

Penalties for violations pertaining to Fraudulent and Unfair Trade Practices (FUTP) during FY 2023 – 2024

796

Adjudication proceedings completed against entities for engaging in FUTP during FY 2023 – 2024

₹5.07 Crore

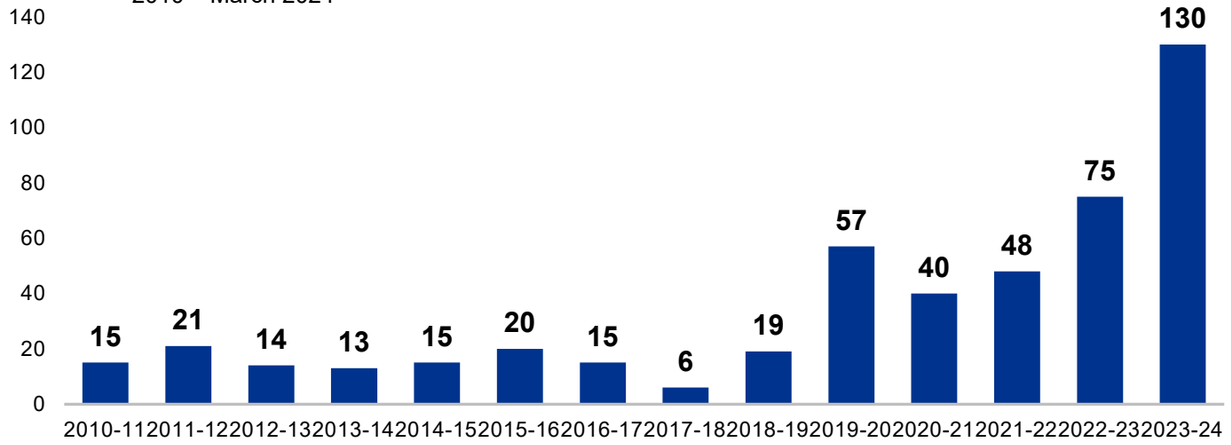
Penalties imposed for involvement in insider trading during FY 2023 – 2024

488

Insider Trading investigations completed by SEBI from April 2010 – March 2024

937

Market manipulation and price rigging investigations completed by SEBI from April 2010 – March 2024



151

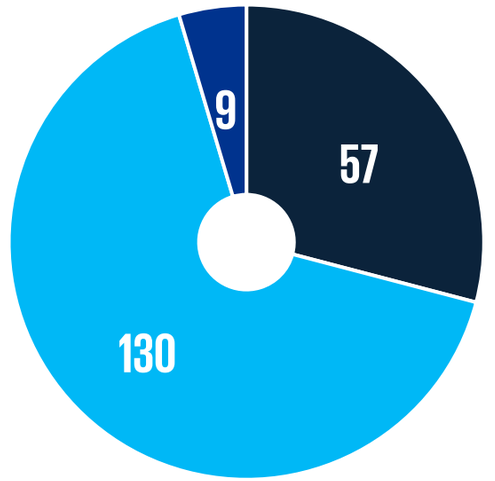
Complaints from investors pertaining to insider trading received during FY 2023 - 2024.

483

Complaints from investors pertaining to price/market manipulation received during 2023 - 2024

197

Investigation cases completed by SEBI in 2023 - 2024



* 55 Entities were fined for violation of SEBI (Prevention of Insider Trading) Regulations, 2015

Source: SEBI Annual Reports for FY 2023-24, FY 2022-23, FY 2021-2022, FY 2020-2021, FY 2019-2020, FY 2018-2019 and 2017-2018 and SEBI Annual Statistics report 2021-2022

Global regulations on insider trading

Insider trading regulations across the globe are designed to uphold market integrity and deter unfair practices. While specific laws and penalties differ, the global approach uniformly emphasises stringent enforcement and severe consequences for violation.

USA Regulations (SEC)

Insider trading definition

As per the USA insider trading rules, "insider trading refers generally to buying or selling a security, in breach of a fiduciary duty or other relationship of trust and confidence, while in possession of material, nonpublic information about the security. Insider trading violations may also include "tipping" such information, securities trading by the person "tipped," and securities trading by those who misappropriate such information.

Penalties

The maximum prison sentence for an insider trading violation is 20 years. The maximum criminal fine for individuals is now $5,000,000, and the maximum fine for non-natural persons is now $25,000,000.

European Union Regulation (Market Abuse)

Insider trading definition

The regulation refers to insider dealing, or insider trading, as a situation where: "a person possesses inside information and uses that information by acquiring or disposing of, for its own account or for the account of a third party, directly or indirectly, financial instruments to which that information relates. The use of inside information by cancelling or amending an order concerning a financial instrument to which the information relates where the order was placed before the person concerned possessed the inside information, shall also be considered to be insider dealing. In relation to auctions of emission allowances or other auctioned products based thereon that are held pursuant to Regulation (EU) No 1031/2010, the use of inside information shall also comprise submitting, modifying or withdrawing a bid by a person for its own account or for the account of a third party."

Penalties

Insider dealing or unlawful disclosure of inside information can attract penalties up to € 5m for natural persons and penalties up to € 15m / 15% of annual turnover for juristic persons.

United Kingdom Regulation (FCA)

Insider trading definition

Under the Criminal Justice Act 1993 (CJA 1993), when in possession of *inside information*, dealing or encouraging another to deal in price-affected securities in relation to that information or disclosing inside information otherwise than in the proper performance of a person's employment, office or profession (*section 52, CJA 1993*)

Penalties

A person convicted of insider dealing under the Criminal Justice Act 1993, on a summary conviction, is liable to a fine or imprisonment for a term of up to 6 months, or both. A person convicted on indictment is liable to a fine or imprisonment for up to 10 years, or both.

Australia Regulations (ASIC)

Insider trading definition

Section 1043A of the Corporations Act 2001 stipulates that a person (referred to as the "insider") must not apply for, acquire, or dispose of financial products or enter into an agreement to do so if they possess inside information or know, or should reasonably know, that the information is inside information. The insider is also prohibited from procuring another person to apply for, acquire, or dispose of financial products or enter into an agreement to do so. Additionally, the insider is prohibited from directly or indirectly communicating the information to another person who they know, or should reasonably know, would apply for, acquire, or dispose of financial products or enter into an agreement to do so.

Penalties

The maximum civil penalties applicable, to individuals is the greater of AUD 1.56 million or three times the profit gained, or loss avoided. The maximum term of imprisonment is 15 years.

For a corporation, the maximum penalty is the greater of AUD 15.65 million or three times the profit gained, or loss avoided or 10 percent of the company's annual turnover in the relevant period.

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 company's 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. Merger, demergers, acquisition, delisting, disposals and expansion of business and such other transactions
5. Changes in key managerial personnel

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 which is deemed as UPSI.

'Generally available Information' means information that is accessible to the public on a non- discriminatory basis, excluding any unverified events or information reported in print or electronic media.

Since all such material events may not be UPSI, companies would have to exercise caution and their own judgment to determine whether events which are material under Regulation 30 of the LODR Regulations, are also likely to materially impact the price of securities, and therefore, be classified as UPSI. While there is no standard formula for determining whether certain information constitutes UPSI, factors such as whether the information has attained a certain degree of finalisation, impact on the decision of a reasonable investor, information related to strategic plans like entering new markets, internal complaints and investigations etc may be considered by the company while deciding whether certain information is price sensitive. Companies should ensure that confidentiality of such information is preserved, which should only be shared 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.

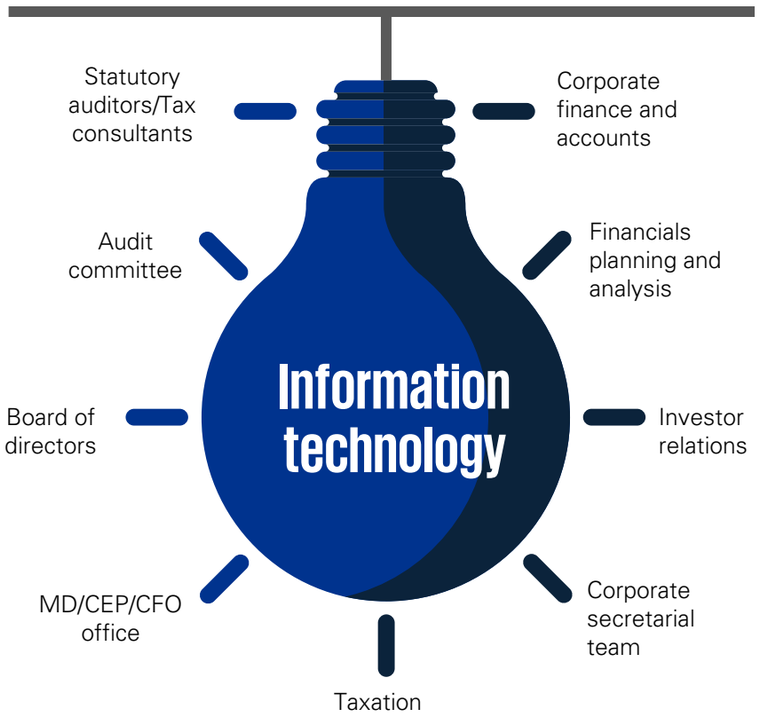
Indicative UPSI list

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

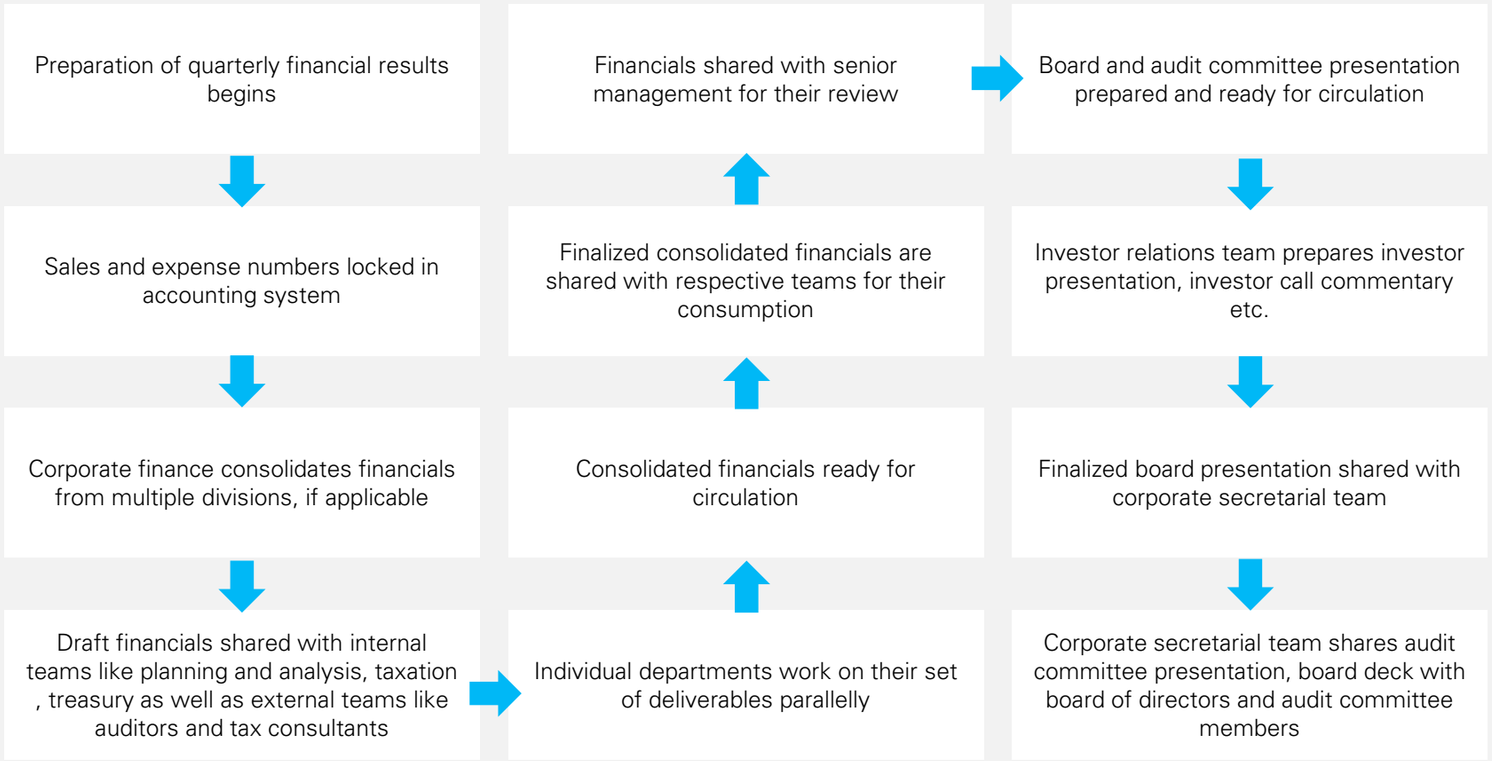
Indicative list of teams handling UPSI

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. 'It must be ensured that the details of all personnel handling UPSI, including nature of UPSI shared, time of receipt, etc., should be suitably recorded in the Structured Digital Database (SDD).

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



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



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

Key challenges faced by companies

As mentioned earlier, technology has made access to data easier. However, it has opened multiple ways in which perpetrators can get access to a company's 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 prohibits 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 person access to UPSI or is reasonably expected to allow such access. Further, the PIT Regulations identifies certain persons as deemed connected persons, such as relatives of connected persons, who would be considered to be an insider.

As required under the SEBI (PIT) Regulations 2015, every listed company is required to frame a Code of Conduct to regulate, monitor and report trading, where certain employees (including their immediate relatives), are specified as designated persons, on the basis of whether their role and function in the organisation provides them access have access to UPSI in addition to their seniority and professional designation. The regulations extend to 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 prevent insider trading.

E

Eavesdropping
Team member overhearing conversations and privy to UPSI information. Many a time work is done in an open office layout and not in control rooms, war rooms or areas with limited or restricted access

Ever connected
Online presence and ability to use various messaging applications which are encrypted, and communication can be monitored by companies.

Espionage
A mole in the team is placed there by competition or third parties for vested interests. Inadequate background checks of outsourced staff or company staff make this a possibility

Extended team
Outsourced vendors, including printers, IT service providers etc. They could have access to the information but may not be covered through PIT coverage defined by the companies.

Emails
Delegation of emails to junior staff and the possibility of information leakage through this channel.

Preserving the confidentiality of UPSI

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, and the details of all persons who share / receive UPSI and nature of UPSI is maintained in the SDD, along with time stamping and audit trails.

In addition to an insider communicating 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. The company should also take measures to ensure confidentiality, such as document control procedures, password-protection systems, etc.

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 a reporting mechanism for violations relating to insider trading and incentivising (up to INR10 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 an 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 unfavourable 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.

Impact of hybrid working model

The rapid outbreak of the pandemic forced companies to rethink on their business perspective by transitioning to a hybrid model. However, this was mirrored by increasing security risks as the transition happened virtually over-night and organisations and employees were not prepared for risk of insider trading and leakage of sensitive information.[5]

With multiple employees working partly from home and partly from office, it has become difficult for companies to ensure compliance to the insider trading policies and procedures. Further, controls and tools implemented by companies to prevent leakages of sensitive information may have become less effective. For instance, it was mandatory to utilise a war room for discussion on unpublished financials while working from office, however these are now being discussed on workspace calls and chats increasing the probability of leakages.

Further, the flexibility to work from home or office has also resulted in rising instances of data breach resulting in leakage of sensitive information. The Ministry of Home Affairs estimated a 300 per cent increase in cyber-attacks on companies in India as compared to 2019.[6]

Companies will also need to re-check on the list of employees to be classified as insiders in accordance with the SEBI (PIT Regulation) 2015. Earlier, the IT personnel responsible for troubleshooting queries were not classified as Insiders. However, with board meetings etc. having migrated to digital platforms, incidental personnel like IT employees may be in possession of un-published price sensitive information.

They key risks of insider trading arising from hybrid model are summarised as follows:

IT risks

- Working remotely increases the use of unsecured online channels and personal devices to conduct e-meetings and share confidential information. Such alternative modes of communication present increasing cyber-security risks as they may not be protected with adequate firewalls to prevent un-authorised access to UPSI.
- Exceptional approval may have been granted by the IT department to select employees to move data to external storage devices and / or share using non-approved IT applications leading to heightened risk of unnoticed leakage of UPSI.[7]

Outsiders related risks

- Companies that are not typically equipped or accustomed to having employees work remotely or in a hybrid mode may have to engage third-party vendors / consultants with access to existing IT infrastructure facilities, as an urgent or emergency measure. Involvement of third parties would increase the operational risk, transactions risk and compliance / regulatory risk. Moreover, these third parties may also have to be covered as insiders who need to comply with company's requirement to prevent insider trading.
- A large number from corporates and intermediaries' employees handling UPSI and working in a hybrid environment creates headroom for leakage of UPSI to family members, friends and others who might have access to shared or virtual working spaces even if un-intentional.[8]

Proposed steps to secure UPSI

- Remind employees to exercise cyber hygiene and ensure adequate IT preparedness to avoid inadvertent cyber-attacks and un-authorised access to UPSI
- Conduct awareness sessions on regulatory requirements to safeguard UPSI and penalties on violation of Insider Trading regulations
- Identify additional employees and third parties who are granted access to UPSI on exceptional basis and impose all restrictions related to designated persons
- Reiterate (and possibly expand) blackout periods and preclearance of trades for designated persons and others in possession of UPSI
- Close monitoring of information leakage from official laptops / mobile phones by optimally using the data leakage prevention (DLP) tools
- Timely withdrawal of administrative rights and/or other exceptional IT privileges extended to select employees, if any
- Minimising circulation of UPSI to attendees and adherence to highest possible standards of data security and confidentiality, while undertaking Board and Audit Committee meetings on digital platforms.

Given the growing vulnerabilities to leakages of UPSI and insider trading violations, it is vital that organisations remain proactive in implementing necessary controls to prevent potential legal, financial and reputational implications.

Considering the ease in which information may be disseminated, all stakeholders should be reminded of the ~~substa~~ntial risks associated with insider trading.[9]

5. Infosecurity Magazine, Insider Threats and Working From Home, [Infosecurity Magazine](https://www.infosecurity-magazine.com/opinions/insider-threats-work-home/).
6. Hindustan Times, Almost 300% rise in cyber-attacks in India in 2020, [Hindustan Times](https://www.hindustantimes.com/india-news/almost-300-rise-in-cyber-attacks-in-india-in-2020-govt-tells-parliament-101616496416988-amp.html).
7. Fortinet, Work From Home Cybersecurity Risks, [Fortinet](https://www.fortinet.com/resources/cyberglossary/work-from-home-cybersecurity-risks).
8. Center for Long-Term Cybersecurity (2022), Security and privacy risks in an era of hybrid work [University of California, Berkeley] (https://cltc.berkeley.edu/publication/security-and-privacy-risks-in-an-era-of-hybrid-work/
9. Suveer Khanna & Mritunjay Kapur, Prime Database, Safeguarding UPSI in a Hybrid Work Model, [Prime Database](https://www.primedatabase.com/article/2020/Article-Suveer%20Khanna%20&%20Mritunjay%20Kapur.pdf).

What is the regulator expecting companies to do?

Recent actions of the regulators clearly show that they are monitoring UPSI leakages, 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 those who manage such controls and periodicity of such reviews including external assessment as appropriate.
- If required, conduct an appropriate enquiry or investigation.

Company's responsibilities in handling UPSI include the following:

- Only the 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 any confidential or sensitive information regarding the company.
- For the preparation, discussion and finalisation of unpublished information, a dedicated room or a virtual set-up with appropriate access controls 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 the setup created.
- Educating all insiders about the sensitivity of information and to restrict disclosures on a '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. It is pertinent to have periodic sessions to reinforce the importance of safeguarding UPSI.

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.

Amend the Code of Fair Disclosures to include policies for determination of the 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, provide 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 a 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 approve and 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 authorised 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 at least 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 maintain appropriate safeguards to maintain confidentiality.
  - Audit committee and Board meetings schedules to be appropriately aligned
  - 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 a structured digital database with details such as persons/entities with whom UPSI is shared. Such database shall be maintained internally with adequate internal controls and checks such as time stamping and audit trails to ensure non-tampering of the database. This requirement of maintaining the database internally was brought in by the SEBI (Prohibition of Insider Trading) (Amendment) Regulations 2020.
  - Investment team/ committee/ research desk of the company has a '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. Appropriate thematic reviews to identify outliers should be conducted on a period basis.
  - All employees involved in handling UPSI should be made aware of closure of trading window and designated persons should take prior approval for trading (as per company stipulated thresholds) while trading window is open. They should also be made aware of contra trade restrictions

Recent judgments

Examining case laws is imperative to understand the severity and implications of insider trading. The following case laws show SEBI's actions against non-compliance and reveal how UPSI was misused.

1. SEBI's interim order in the matter of suspected Insider Trading in leading dairy company (Order date: 14 May 2024):[10]

Background of the case:
The Securities and Exchange Board of India (SEBI) initiated an investigation into allegations of price manipulation in the scrip of the dairy company. The investigation primarily focused on Mr. SD, the promoter and managing director of the company, who was found to have executed contra trades and engaged in trading during periods when the trading window was closed. These activities were identified as violations of SEBI regulations, prompting further scrutiny and subsequent legal actions.

Events leading to Insider Trading
The investigation covered the period 1 March 2018 to 31 July 2018. During this time, Mr. SD bought 4,460,225 shares and sold 20,330,184 shares of the dairy company, which were identified as contra trades. These transactions led to a profit of INR2.12 crores; a sum that was not remitted to SEBI, as required by the regulations. Additionally, Mr. SD undertook trading during a closed trading window, i.e., sold 9,068,710 shares valued at INR22.14 crores. This activity was in direct violation of SEBI's insider trading regulations, which prohibit trading during such closed periods to prevent the misuse of unpublished price sensitive information.

Penalties and actions taken
In response to these violations, SEBI ordered Mr. SD to disgorge the profit of INR2.12 crores obtained from the contra trades. Furthermore, a monetary penalty of INR 0.10 crores was imposed. To ensure compliance, SEBI prohibited Mr. SD from disposing of or alienating any assets until the disgorged amount and penalty were fully deposited with SEBI. These actions were taken to uphold the integrity of the securities market and ensure that violations of insider trading regulations were appropriately penalised.

2. SEBI's order on the Insider Trading of leading producer and exporter of aquaculture products (Order date: 28 March 2023):[11]

Background of the Case:
A leading aqua food company, an integrated producer and exporter of aquaculture products disclosed its financial results for the quarter ended 30 September 2017, on 14 November 2017, revealing a significant profit increase from the previous quarter. This announcement caused a substantial rise in the company's stock price, prompting an investigation by the Securities and Exchange Board of India (SEBI).

Events leading to Insider Trading:
SEBI's investigation focused on trading activities between 4 September 2017, and 28 February 2018. The investigation identified that key insiders, including Mr. SK (Promoter, Chairman, and Managing Director), Ms. PK (Promoter), and Mr. RK (son-in-law of the promoter), traded the company's stock based on UPSI. The financial results, which constituted UPSI, were known to company's key management personnel before the official disclosure. This period, from 3 October 2017 to 14 November 2017, was identified as the UPSI period. During this time, Mr. SK and Ms. PK made substantial purchases of the company's shares.

Penalties and actions taken:
SEBI's investigation concluded that key insiders of the company were engaged in insider trading based on UPSI. As a result, Mr. SK, the company's Promoter, Chairman, and Managing Director, was found guilty of purchasing 23,500 shares during the UPSI period, resulting in unlawful notional gains of INR0.15 crores. SEBI imposed a penalty, directed disgorgement of these unlawful gains and imposed a ban on trading in securities. Ms. PK, another promoter, was also found guilty of purchasing 70,183 shares based on the UPSI communicated by Mr. SK and faced similar penalties, disgorgement, and a trading ban.

3. SEBI vs. AR (C.A. No. 563/2020) decided by Supreme Court of India (Order date: 19 September 2022):[12]

Background of the case:
Mr. AR served as the Chairman and Managing Director of a leading infrastructure company when the National Highways Authority of India (NHAI) awarded significant contracts to the company. The company along with another leading infrastructure company had entered into two shareholders agreements, which were subsequently terminated by the Board on August 9, 2013. Prior to the public disclosure of this termination on August 30, 2013, Mr. AR sold shares on August 22, 2013. Following an investigation, SEBI found Mr. AR guilty of insider trading under the 1992 regulations and ordered him to disgorge the unlawful gains.

Judgement:
The Supreme Court examined the definition of "price-sensitive information" under clause (vii) of regulation 2(ha) of the 1992 regulations, determining that the information in question fell within this clause. The Court emphasised that clause (vii) is distinct from clauses (i) to (vi), as it is broad and general in nature. Thus, it cannot be presumed to materially affect security prices unless explicitly demonstrated.

Factually, the Court found that Mr. AR's trade was intended to prevent the bankruptcy of the leading infrastructure company's parent company. The Supreme Court was further influenced by the fact that the nature of the price-sensitive information did not align with the intention to exploit the situation for personal gain. By selling the shares before the public disclosure of the information, Mr. AR did not act to benefit from insider knowledge, indicating that his actions were not driven by "normal human conduct" as typically understood in cases of insider trading.

10. "Securities and Exchange Board of India v. SD, Case on Insider Trading in Dairy Company, SEBI Order, 2018." Link: [SEBI Order 2018](https://www.sebi.gov.in/orders/dairy-company-insider-trading-case.pdf).
11. "Securities and Exchange Board of India v. SK, Insider Trading Case on Aquaculture Company, SEBI Ruling, 2019." Link: [SEBI Aquaculture Case](https://www.sebi.gov.in/orders/insider-trading-aquaculture-case.pdf).
12. "AR v. SEBI, C.A. No. 563/2020, Supreme Court of India, 2020." Link: [Supreme Court Judgment] (https://api.sci.gov.in/supremecourt/2020/1791/1791_2020_4_1501_38300_Judgement_19-Sep-2022.pdf)

Recent judgments

4. BG v. SEBI (C.A. No. 7054/2021) decided by Supreme Court (Order date: 19 April 2022):[13]

Background of the Case:
The legal case of BG v. Securities and Exchange Board of India (SEBI) centered on allegations of insider trading against the Chairman and Managing Director of a publicly listed company and their immediate family members. SEBI, the regulatory authority overseeing Indian securities markets, alleged that these individuals shared Unpublished Price Sensitive Information (UPSI) with their family members, who subsequently traded securities based on this privileged information. Central to the dispute was SEBI's ability to substantiate these insider trading claims with sufficient evidence.

Issues raised:
Whether the Chairman and the Managing Director had indeed conveyed UPSI to their relatives, thus violating insider trading regulations?

Whether the relatives qualified as immediate relatives within the meaning of the Regulations, or whether they had engaged in trading while being in possession of UPSI?

Judgement:
Insufficiency of circumstantial evidence: The court highlighted that circumstantial evidence, such as trading patterns and timing, was insufficient on its own to establish guilt in insider trading cases. SEBI bore the burden of proving not only communication between the Chairman/Managing Director and their relatives but also that the relatives possessed UPSI at the time of their trades.

Classification of immediate relatives: In determining whether the relatives qualified as immediate family members under regulatory definitions, the court examined factors including financial independence, estrangement from the Chairman/Managing Director, and their resignation from company positions. Based on these considerations, the court concluded that the relatives did not meet the criteria of immediate relatives as per regulatory standards. Consequently, they were not considered connected persons presumed to have access to UPSI.

13. "BG v. Securities and Exchange Board of India, C.A. No. 7054/2021, Supreme Court of India." https://api.sci.gov.in/supremecourt/2021/26746/26746_2021_9_1501_35070_Judgement_19-Apr-2022.pdf

Conclusion

Securing UPSI and ensuring that the data doesn't fall in the 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 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:

- Implement data leakage prevention solutions, IP-based access controls, blocking of emails containing key words, and restricted usage of mobile phones in the dedicated room or in public places to discuss UPSI.
- Avoid storing sensitive data over the 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 of what can be identified as 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 workspace with secured access for teams working on preparing the financials of the company 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
- Proactively monitor any significant price changes just before the declaration of financial earnings for any significant fluctuations.

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.

Self-assessment questionnaire

1. UPSI identification

Does your company have a clearly defined list of information that qualifies as Unpublished Price Sensitive Information (UPSI)?

☐ **Yes** ☐ **No** ☐ **Don't Know**

2. UPSI handling protocols

Are there documented protocols specifying the steps to be followed when UPSI is received or generated within your company?

☐ **Yes** ☐ **No** ☐ **Don't Know**

3. UPSI access control

Is access to UPSI restricted to a specific group of employees with a legitimate need, and is this access regularly reviewed? Also, does the company frequently update its IT infrastructure to strengthen internal controls and prevent leakage of unpublished price sensitive information (UPSI)?

☐ **Yes** ☐ **No** ☐ **Don't Know**

4. UPSI communication restrictions

Does your company have a policy that prohibits the sharing of UPSI through unsecured communication channels (e.g., personal emails, unencrypted messages)?

☐ **Yes** ☐ **No** ☐ **Don't Know**

5. UPSI in public interactions

Are there specific guidelines for employees on how to avoid inadvertently sharing UPSI during public interactions, such as investor meetings or media interviews?

☐ **Yes** ☐ **No** ☐ **Don't Know**

6. UPSI disclosure management

Is there a documented procedure for obtaining approval from the compliance/legal team before disclosing any UPSI to external parties?

☐ **Yes** ☐ **No** ☐ **Don't Know**

7. UPSI monitoring and logging

Does your company use monitoring tools to log and review access to UPSI to detect any unauthorised access or unusual activities? Are there access controls in place to ensure only authorised personnel can access the Structured Digital Database (SDD)?

☐ **Yes** ☐ **No** ☐ **Don't Know**

8. UPSI breach response plan

Has your company established a response plan for potential breaches of UPSI, including specific actions to mitigate damage and report the incident?

☐ **Yes** ☐ **No** ☐ **Don't Know**

9. Employee declarations

Are employees required to declare their understanding of the UPSI policy and confirm their compliance with it annually?

☐ **Yes** ☐ **No** ☐ **Don't Know**

10. UPSI awareness for contractors and consultants

Does your company extend UPSI policies and training to contractors, consultants, and other third parties who might have access to UPSI?

☐ **Yes** ☐ **No** ☐ **Don't Know**

11. UPSI incident reporting

Is there a formal process in place for employees to report potential breaches or incidents involving UPSI, and are they encouraged to do so without fear of retribution? (Can club with UPI breach response plan)

☐ **Yes** ☐ **No** ☐ **Don't Know**

12. UPSI documentation retention

Does your company have a policy outlining the duration for which UPSI documents should be retained, as well as the secure disposal process for such documents when they are no longer required?

☐ **Yes** ☐ **No** ☐ **Don't Know**

13. Legal and regulatory compliance

Does your company regularly review and update UPSI handling protocols to ensure compliance with relevant legal and regulatory requirements?

☐ **Yes** ☐ **No** ☐ **Don't Know**

14. External communication Audit

Are there periodic audits or reviews conducted to ensure compliance with UPSI communication restrictions and to verify that external communications involving UPSI adhere to company policies?

☐ **Yes** ☐ **No** ☐ **Don't Know**

15. UPSI annual awareness training

Are UPSI awareness training conducted for employees annually?

☐ **Yes** ☐ **No** ☐ **Don't Know**

16. Stakeholders for UPSI annual awareness training

Which categories of personnel and stakeholders are earmarked for the annual UPSI awareness training?

☐ **Board of Directors** ☐ **KMP and designated person** ☐ **All employees**

Acknowledgements

Analysis and content:

Suveer Khanna
Mustafa Surka
Sudesh Anand Shetty
Siddharth Gautam
Tanmay Bhargava
Geetu Singh
Kirit Amichandwala
Karan Marwah
Aditya Lahoti
Muntazar Sayed
Inayat Sistani
Meenakshi Sharma
Manan Doshi
Jaykishan Motwani
B Balaguhan
Ayush Menon
Anjali Dhawan
Isha Bhattad

Design team:

Angeeta Baweja

Marketing compliance team:

Pooja Patel

KPMG in India contacts

Akhilesh Tuteja
Head
Clients & Markets
E: atuteja@kpmg.com

Manoj Kumar Vijai
Partner and Head
Risk Advisory
E: mkumar@kpmg.com

Suveer Khanna
Partner and Head
Forensic Services
E: skhanna@kpmg.com

Karan Marwah
Partner and Head
Capital Markets
E: kmarwah@kpmg.com

Sudesh Shetty
Partner
Forensic Services
E: sashetty@kpmg.com

Muntazar Sayed
Technical Director
Forensic Services
E: muntazarsayed@kpmg.com

Finsec Law Advisors contacts

Sandeep Parekh
Managing Partner
E: Sandeep.parekh@finseclaw.com

Anil Choudhary
Partner
E: anil.Choudhary@finseclaw.com

Rashmi Birmole
Senior Associate
E: rashmi.birmole@finseclaw.com

home.kpmg/in

Access our latest insights
on KPMG Insights Edge

Follow us on:
kpmg.com/in/socialmedia