Menace of Insider Trading in the 'new normal'

Mritunjay Kapur
Executive Director-Head of Advisory, KPMG in South Africa & Board Member
KPMG in India

Suveer Khanna
Partner, Forensic Services
KPMG in India

The COVID-19 pandemic is significantly changing the ways corporates, their employees and third-party service providers are coping to keep up with business continuity. The significant volatility in business conditions have caused some organisations to struggle to keep as going concern issue; while others into running a brisk demand for their goods and services and growing significantly. As Corporate India tries to adapt to the 'new normal', it is certain that our securities markets continue to battle old problems in a new garb.

When the nation-wide lockdown was imposed a few days before the end of 31 March 2020 fiscal year, a significant amount of Unpublished Price Sensitive Information ('UPSI') related to financial results, was in the process of being finalised. Securities and Exchange Board of India ('SEBI') issued a circular dated 30 June 2020, which provided relaxations from the compliance requirements during COVID-19, allowing financial results to be filed by 31 July 2020. The problem of insider trading was thus aggravated by the fact that the trading window closures would be automatically delayed for another two months, unless those were specifically exempted by the regulator.

Many 'insiders' during this period would have had access to UPSI pertaining to key performance standards such as, financial transactions, business disruptions, material contracts, mergers or acquisitions, etc. These 'insiders' could have also had information on how the pandemic impacted other entities, including customers, vendors, merchants and other third parties, with which their organisation interacted on a regular basis. This nature of information would have allowed insiders to foresee and anticipate unexpected benefits and hence plan their trading and make allocation decisions efficient. The situation created a lucrative opportunity for insiders, who regularly have access to UPSI, that held an even greater value under the 'new normal', than under pre COVID-19 times.

Under the 'new normal' working from home has become inevitable, Senior Management and Board meetings have gone virtual leading to distribution of UPSI into dozens if not hundreds of geographical locations without the same level of physical and visual checks to protect it from leakages. These chaotic circumstances posed not only a threat of loss of income to various individuals (e.g., job losses, salary cuts, etc.), but also the perfect opportunity for unscrupulous 'insiders' with slippery ethical values, to access the UPSI. Together, these factors create unique and unprecedented opportunities for insider trading. In short, all the three elements of the fraud triangle – incentive, opportunity and rationalization, co-exist together.

With remote working becoming more prevalent in the 'new normal', the risks pertaining to leakage of UPSI have also evolved in today's environment due to various reasons as listed below:

1. **Eavesdropping**: While the risk of eavesdropping existed during the pre- COVID times, it has amplified as employees with access to UPSI are working remotely. With working from home becoming the 'business as usual' and key business meetings having gone virtual, the risk of 'accidental tipping' to family members, friends and others, is bound to rise.
2. **Espionage**: Remote working has led to digitization of many activities such as, meetings of Senior Management, Board, Audit Committee and other important meetings, which were held in the confines of a board room, moved to various collaboration tools under the 'new normal'. Recent reports indicate that there has been significant rise of cyber-attacks on collaboration applications, leading to leakage of information discussed during these meetings. From installation of 'bugs' in office spaces, perpetrators have moved to manipulating user(s) to install desktop or sharing apps with an intent to get remote access to the information.
3. **Extended teams**: The recent work from home mandate, has dramatically changed how we work. To provide the Information Technology ('IT') infrastructure to meet the demands of remote working, organisations that were not typically equipped with working remotely, have to engage additional third-party vendors/consultants, with

privileged access to existing IT infrastructure facilities, as an urgent or emergency measure. Involvement of third parties increase operational risk, transaction risk and compliance/regulatory risk. Often it is noted that the IT teams have access to UPSI, but are not classified as 'insiders' by organisations, thereby increasing the risk of leakage of UPSI.

4. **Ever connected**: Most employees working remotely, are accessing their organisation's data and networks, even though they are not protected by their organisation's secure IT infrastructure. The financial fraudsters/ cyber criminals are on the prowl, preying on the many rendered as emotionally and financially vulnerable. The fraudsters are employing many methods — some new and some time-tested. They are also quick, using day-to-day developments. The game plan is to make the employee part with information or to install malware in their electronic devices to thieve information.
5. **Emails**: Business email compromise is a huge threat with everyone working remotely. There has been a rise in spear-phishing attacks, that typically involve an employee being convinced to make a change in a standard business process. The perpetrators set up a domain very similar to the corporate domain which have certificates issued, so everything appears to be right. The perpetrators begin sending out email messages stating that there are adjustments to the cloud email infrastructure and as a part of this, they need the employee to reset the access credentials by clicking on the link included. When the employee falls for this, the perpetrators gain access to their email. In effect, the targeted employee becomes the man-in-the-middle between all incoming and outgoing emails. This helps the perpetrators gain access to all the sensitive information of the organisation.

Initiatives to secure UPSI

In order to protect themselves from insider trading or any enforcement action, organisations should take precautionary measures such as evaluating their internal controls and revising the insider trading policies of the organisation, thus ensuring that these policies are clearly demarcating the prohibition of trading on UPSI and adequately addressing the increasing opportunities for such trading that might have been created due to the pandemic. In addition, some of the initiatives that organisations could adopt to secure UPSI are as follows:

- Assess the processes under the 'new normal' to identify areas where the UPSI is more at risk of getting leaked.
- Maintain a structured digital database containing the nature of UPSI and the names of persons who have shared such crucial internal information.
- Minimise circulation of UPSI to attendees and adhere to highest possible standards of data security and confidentiality, while undertaking Board and Audit Committee meetings, on digital platforms.
- Close monitoring of information leakage from official laptops/mobile phone by optimally using the data leakage prevention ('DLP') tools. Consider making information virtual (e.g., paperless environment), without download rights, use of camera, etc.
- Identify additional employees and third parties who are granted access to UPSI on exceptional basis and impose restrictions related to 'Designated Persons'.
- Timely withdrawal of administrative rights and/or other exceptional IT privileges extended to select employees during the lockdown, if any.
- Reiterate (and possibly expand) blackout periods and preclearance of trades for Designated Persons and others in possession of UPSI.
- Remind employees to exercise cyber hygiene and ensure adequate IT preparedness to avoid inadvertent cyberattack and unauthorised access to UPSI.
- Conduct awareness sessions on regulatory requirements to safeguard UPSI and penalties on violation of the Prevention of Insider Trading ('PIT') regulations.

Securing UPSI and ensuring that confidential data does not fall in the wrong hands is critical for an organisation to ensure continued investor confidence, preserving its own reputation and goodwill in the market. Given the growing vulnerabilities to leakages of UPSI and insider trading violations, it is vital that organisations remain proactive in implementing necessary controls and good practices such as investing in the right processes, right technology and people control to prevent potential legal, financial and reputational implications.