International Journal of Law Research, Education and Social Sciences

Open Access Journal – Copyright © 2026 – ISSN 3048-7501
Editor-in-Chief – Prof. (Dr.) Vageshwari Deswal; Publisher – Sakshi Batham

Tracing the Trail: Digital Evidence and the New Era of Insider Trading Regulation

Anand Kumar Bose[a] Amaan Ahmed[b]

[a]Ideal Institute of Management and Technology and School of Law, GGSIPU, Delhi, India [b]Ideal Institute of Management and Technology and School of Law, GGSIPU, Delhi, India

Received 04 March 2026; Accepted 03 April 2026; Published 07 April 2026

As of now, the rules and enforcement surrounding insider trading regulation and enforcement have become stricter (2023–2025) due to the increased use of electronic communications as evidence, the narrowing of safe harbours for transactional evidence, and more stringent standards for what constitutes sufficient disclosure and pre-clearance. Recent changes to the rules and guidance regarding insider trading regulations and enforcement, predominantly from the SEC and FCA and recent supervisory developments from ESMA and SEBI, illustrate that all regulatory authorities expect that the documentation and archive of both on- and off-channel communications will be robust and that the procedures for good-faith when trading plans or due diligence exceptions are invoked will be demonstrable. The enforcement, including the conviction of Terren Peizer and the cross-border enforcement for trading on top of encrypted-message metadata, demonstrates that formal trading plans, post-hoc disclosures, or sparse notification are of little consequence in light of the digital record and timing of events that diminished the defences of those trading. Compliance functions must thus enhance their pre-clearance processes, tighten their governance around trading plan (cooling-off period and anti-overlap rules), require "sufficiently detailed" trade notices, and develop the archival and surveillance capabilities necessary to develop a defensible, supportable audit trail. The net outcome of this is that while there are still safe harbours available, they have become restrictive; and with there being insufficient processes, records, and digital-communications controls, the risk for all parties involved has increased substantially.

Keywords: *insider trading, pre-clearance procedures, sufficiently detailed disclosure, due diligence safe harbour.*

INTRODUCTION

Insider trading is a form of malpractice that occurs when people use information that others don't have to gain an unfair advantage. This information was leaked by someone inside the company, giving unfair advantages to those using it. Insider Trading is an illegal practice. Insider trading laws are becoming stricter worldwide. The administration which makes specific laws about Securities are making more precise laws by strictly examining the digital communication, closing any plotholes like "pre-clearance" trading plans and demanding of SDD(sufficiently detailed disclosure) it is an application which is required in patent law and sometimes in finance, which must describe the invention(creation) or the situation, which can help another skilled person do three important things like understanding it, replicate it and make any informed decision without any experiment of their own, SDD of trades are checked by the Administration. In the U.S., the SEC's (Securities and Exchange Commission) 2023 rules on new disclosure and cooling-off related to Insider Trading. In Europe, the 2024 EU Listing Act amended the Market Abuse Regulation(MAR) to expand the safe-harbours(e.g., buy-back shares) and provide some relaxation delays on disclosure. India's SEBI in 2024 gave relaxation on trading plan rules, reducing cooling-off periods and completely removing the minimum plan lengths. Across jurisdictions, enforcement actions generally rely upon evidence like emails, WhatsApp texts, and trading logs, as observed in the high-profile matters of the UK to the US. Firms and directors cannot assume safe-harbour protection unless they thoroughly comply with the policies; pre-clear trades, full detailed disclosures and have all relevant communication.

Main points: Financial regulators across the globe (SEC, FCA, ESMA, SEBI, etc.) have established new rules and procedures to tighten insider-trading controls (2023–2025), and recent actions taken show that email/text records and 10b5-1 plans are being reviewed.[1] Abuse will be a major enforcement issue. Best-practice procedures at this time require strong pre-clearance policies and procedures, surveillance in real-time (which also includes off-channel communication), and detailed documentation. The following chart provides a comparative

[1] Commodities and Securities Exchange (17 C F R) pt 240.10b5-1; 'SEC Adopts Amendments to Modernize Rule 10b5-1 Insider Trading Plans and Related Disclosures' (*Securities and Exchange Commission*, 14 December 2022) <https://www.sec.gov/news/press-release/2022-222> accessed 03 March 2026

overview of the various regimes of insider trading in the US, UK, EU, and India. In addition, there is a timeline of recent developments noted, and a compliance checklist outlining the steps firms can take to be compliant.

UPDATES IN REGULATION(2023-2025)

US (SEC/DOJ): Insider trading continues to be a top priority for both the SEC and the DOJ. In November 2022, the SEC adopted significant changes to Rule 10b5-1 (which will be effective February 27, 2023), requiring all trading plans to include a cooling-off period, certifying that participants have no material non-public information ("MNPI"), preventing the submission of overlapping plans, and disclosing all such plans before commencement and trading of securities in connection with such plans. In addition, issuers will now need to disclose all trading plans and associated trading activity on SEC Forms 10-Q[2]/10-K[3] and 4/5. The SEC guidance speeches and Enforcement Reports issued between 2023 and 2025 will continue to specifically point out that both fraud involving digital assets and off-channel (unarchived) digital means of communication (SMS/texts, Slack, etc.) will be the primary enforcement focus. For instance, the SEC Chair has publicly announced that the Office of the Chair intends to focus on violations of recordkeeping relative to text messaging and that the Acting Chair of the SEC (Gurbir Grewal) will announce a renewed focus on violations of "core frauds" (including insider trading) through 2025. In 2024, the U.S. Supreme Court reaffirmed existing rights of defendants via the Jarkesy ruling[4] while leaving the substantive law regarding insider trading unchanged.

UK (FCA): The FCA has increased the pace of anti-market abuse enforcement exponentially. Recent FCA statistics (2024/25) reveal an increase in investigations and enforcement action against insider trading (for ex, 29 new investigations between 3/2024 – 10/2024). Numerous FCA speeches (April 2025) outline an anti-market abuse strategy with a particular focus on insider dealing. As of October 2023 and continuing, the FCA has been very active in enforcing insider-related cases, including successfully prosecuting foreign nationals for trading on insider

[2] 'FORM 10-Q' (*Securities and Exchange Commission*) <https://www.sec.gov/about/forms/form10-q.pdf> accessed 03 March 2026
[3] 'Form 10-K' (*Securities and Exchange Commission*) <https://www.sec.gov/files/form10-k.pdf> a accessed 03 March 2026
[4] *SEC v Jarkesy* [2024] 603 U S 109

information as well as placing large Fines against companies whose internal communications and/or trading policies failed to identify the trading of insiders.

The FCA has issued Best Practices and guidance to its staff, reminding firms that their employees must pre-clear all trades and that leaking material nonpublic information must be managed tightly (see sidebar note). The FCA has also issued numerous Practice Notes, such as the "Inside Information" Practice Note (initially issued in 2020 and last updated in January) and the 2024 "UK Listing Review" (both of which emphasised the establishment of enhanced transaction-related disclosures and the need for firms to have robust systems and controls).

EU (ESMA): The European Union has amended the EU Market Abuse Regulation via Regulation 2024/2809 (Listing Act), effective December 4, 2024. The changes include amending Article 5 (safe-harbour)[5] for issuers of their own share buyback and amending Article 19 (increasing the notification threshold required for managers trading).[6] The Act also broadens the permitted legitimate interests for being able to delay disclosures (e.g., the Regulator requesting not to disclose or simultaneous bids from multiple bidders), as well as repealing the historic rule allowing no outside representation or creating misleading information to the public. The European Securities and Markets Authority (ESMA) has begun consulting on (2/2026) expanding its guidelines for insider information to better reflect changes resulting from the Act. ESMA and National regulators such as BaFin and FIN-FSA continue to restate that market sounding (communication with potential customers), buybacks (purchases made by an issuer of its own stock), and high-frequency trading are subject to specific safe harbour provisions, while no additional uses of MNPI (Material Non Public Information) are acceptable.

India (SEBI): The approach that India's SEBI took was quite different; in June 2024, SEBI relaxed the insider trading regulations to better facilitate market liquidity. The recent amendments(effective September 23, 2024) to Section 29 (Trading plan provisions) of the SEBI (Prohibition of Insider Trading) Regulations 2015[7] result in new deregulated provisions as follows; (a) the hold period to execute a trading plan will be reduced to 120 days from 6 months;

[5] Regulation (EU) 2024/2809 of the European Parliament and of the Council of 23 October 2024 amending Regulations (EU) 2017/1129, (EU) No 596/2014 and (EU) No 600/2014 to make public capital markets in the Union more attractive for companies and to facilitate access to capital for small and medium-sized enterprises OJ L 2024/2809, art 5
[6] *Ibid* art 19
[7] Securities and Exchange Board of India (Prohibition of Insider Trading) Regulations 2015

(b) the minimum hold period will be eliminated and (c) limit orders will now be permitted within a trading plan; therefore, it will allow more flexibility for designated insiders (Key Management Person and promoters) executing a plan to trade. SEBI maintains strict regulations for disclosure and pre-clearance; however, all insiders are required to pre-clear their transactions and report their trades in any dollar amount to the issuer within two days of trading (the issuer must then announce it to the exchange). Furthermore, SEBI has been very aggressive in their efforts to investigate the misuse of price-sensitive information (for example, monitoring advisors' networks to detect tippees from social media).

Regulatory Authority Within Various Jurisdictions. Several jurisdictions have reaffirmed their strict view towards the use of encryption in communications, ie, encrypted chat messaging. For instance, the Hong Kong SFC and Singapore MAS have both recently taken action against the misuse of encrypted chat messaging. The FSA in Japan has issued guidance to managers on the use of an ethical code for managers. Similarly, the ASIC in Australia is indicating that firms must record and maintain archived copies of all channels of communication as part of their record-keeping obligations. Key points related to the U.S., U.K., E.U. and India are summarised at the end of this document.

IMPORTANT CASES

Encrypted Chats/Communications: Cross-Border Schemes (United States): USA v. Khouadja, 2026[8] (D. Mass) prosecutors outline a 10-year-long, multi-national insider trading conspiracy in connection with M&A deals involving Europe; defendants referred to "burner phones" and used encrypted applications (ie. Signal, WeChat, Telegram, etc.) to communicate trade "tips" and transmit payments related to insider trading; prosecutors' knowledge is based on details included in the indictment related to several years of wiretaps and mutual legal assistance; attorneys for the U.S. Attorney's office in Massachusetts have utilized "cloud backup data of encrypted messages that the defendants believed would be impossible to determine to assist in bringing these matters to closure." All of these provide compelling evidence that no

[8] *United States v Khouadja et al* [2025] Case No 1:24-cr-10200-RGS (D Mass); 'Eight Members of Global Insider Trading Network Charged With Securities Fraud and Money Laundering Offences' (*Department of Justice*, 18 November 2025) <https://www.justice.gov/usao-ma/pr/eight-members-global-insider-trading-network-charged-securities-fraud-and-money> accessed 03 March 2026

communication is absolutely private; even very complex encryption methods (ex, "socks" for SIM cards) may be circumvented by contemporary forensics.

10b5-1 Trading Plans (US): In June 2024, after a jury found the ex-CEO of a public company (Terren Peizer) guilty of insider trading, he used 10b5-1 plans, which had been in place to facilitate the execution of illegal trades. He had created two trading plans shortly after receiving material, non-public information about his company without disclosure. He subsequently liquidated shares quickly and avoided an estimated $12.50 million in loss through the execution of these plans. While the execution of these plans was officially recorded, Peizer could still be prosecuted for insider trading because the judge allowed the prosecution to introduce evidence to prove that he had knowledge of the MNPI when the plans were created. The US law firms have characterised this prosecution as being the "first criminal conviction based solely on using Rule 10b5-1 plan(s)." The US Department of Justice has since warned that if a company created a planned schedule for the execution of a trading plan in bad faith, they would be liable for prosecution as well. The Securities Exchange Commission for the US has also initiated a parallel civil action against Peizer. Lesson: Companies must scrutinise when they adopt trading plans and certify them in accordance with the law.

Off-channel communications (UK): In 2025, the UK Financial Conduct Authority (FCA) enforced a £309,843.00 civil action against Russel Gerrity for a series of WhatsApp messages that were sent while he was onsite executing bidding on behalf of a public energy company. This series of communications indicated that Gerrity had non-public knowledge of a particular company's bidding intentions and further indicated that the bid would be issued. More broadly, FCA employees have identified the risks associated with the use of messaging applications for conducting any communications that involve material, non-public information. According to a 2024 multi-firm study, there is overwhelming evidence of a rise in insider leaks through private group chats and texting. In addition, both in the UK and outside of it, suspicious trading has occurred using Slack, Discord and even DMs on Twitter.

Examples of Pre-Clearance and Compliance Problems: As illustrated in the recent BIDSTACK (2026)[9] case, an interim Chief Financial Officer (CFO) leaked material non-public

[9] 'FINAL NOTICE: Bhavesh Hirani' (*Financial Conduct Authority*, 27 January 2026) <https://www.fca.org.uk/publication/final-notices/bhavesh-hirani-2026.pdf> accessed 03 March 2026; 'FINAL

information about a pending merger to a friend, who executed trades from a brokerage account registered in the name of that friend; the trades were placed entirely outside the company's pre-clearance process but were detected by trade surveillance and subsequently reported to the Financial Conduct Authority through a Suspicious Transaction Report ("STR").

In another example out of the UK, the Financial Conduct Authority (FCA) banned and fined Poojan Sheth and Diego Urra (JP Morgan investment bankers) for leaking insider tips to a trader and for being complicit in passing along unapproved pre-trade information based on their internal text messages and emails. These examples illustrate that if insiders fail to comply with the company's pre-clearance processes by trading outside of its authorised brokerage accounts or by creating unauthorised brokerage accounts, such transactions will be identified through modern trade surveillance.

Global Research Literature: Law firms and academia have noted that, even in jurisdictions considered to be friendly to the use of technology (e.g., Singapore and India), there is an explosion in the storage and use of digital diaries and records of text, messaging and messaging metadata and trading analytics. As a result, investigations typically include requests for corporate telephone records, email logs and corporate backups of employees' WhatsApp communications.

SDD(SUFFICIENTLY DETAILED DISCLOSURE)

The term "sufficiently detailed disclosure" applies to the need for insiders' trades – and an issuer's announcement of a trade – to be disclosed with the full facts about the transaction so that the market can assess it. Under the EU and UK rules, a PDMR must notify an issuer of his or her own trades as soon as reasonably possible (UK: within three business days, EU: similar). The issuer must then publicly announce the trade within four business days, giving the name of the trader, the date, the type of the trade, and the volume of the traded instrument, the price, and the nature of the trade.

UK Listing Rule 9.6.3R[10] states that these announcements must be sufficiently detailed to enable investors to understand them. Guidance from the regulator has stated that sparse

NOTICE: Dipesh Kerai' (*Financial Conduct Authority*, 27 January 2026) <https://www.fca.org.uk/publication/final-notices/dipesh-kerai-2026.pdf> accessed 17 March 2026

[10] UK Listing Rules 2024, r 9.6.3

announcements may result in violations of obligations to maintain an appropriate level of transparency. Issuers should explain the reasons for a transaction (e.g., exercise of options, market sell-off, etc.) if it may materially impact the manner in which the transaction is viewed.

Regulators have made more pronounced calls for increased issuer disclosure. The FCA, in its 2024 Listing Review, has proposed a "sweeper" disclosure rule that would require issuers to add additional relevant context to allow shareholders to evaluate any transaction. This focused on acquisition transactions and a culture of over-disclosure. Similar to the ESMA Q&A Updates (Dec 2025), the Market Abuse Regulation states that inside information must have no missing material facts in the release from the issuer. Therefore, companies are responsible for having their insiders trained on providing all the factual information when notifying their trades. Regulators can penalise a company if a release does not include details, such as stating a volume change only, without stating whether it was a sale.

Enforcement can also rely on the date of the prior announcement (SDD). An insider may claim to be unaware of something by referencing a public announcement made in advance, and the authorities will review that public announcement for any omissions. Under the EU Listing Act, delayed disclosures can only occur if the delayed disclosures do not correspond with a prior announcement. As a result, a small pre-disclosure number followed by an insider's quiet trade can raise suspicions about stock "ramping".

DIGITAL EVIDENCE AND OFF-CHANNEL COMPLIANCE

The ease of access to electronic devices has led to a paradigm shift in the way electronic evidence is obtained for insider trading. For example, surveillance equipment has been deployed to identify suspicious trading patterns and then allow investigators to further an investigation through communication channels. Any type of communications that suggest a foreknowledge of coming good news can now be obtained by the use of a subpoena. The SEC has publicised both the analysis of trading data and the enforcement of the laws related to insider trading – the Commission's FY 2023 annual report provided numerous examples of insider trading investigations that were initiated as a result of the analysis of trading data. Similar support for the use of trading data and electronic communications (e.g., Suspicious Transaction Reports and whistleblower testimony) has been given by the FCA and ESMA.

As a result of these developments, companies must manage their electronic records effectively. Best practice now requires that all work-related communications (including emails, Bloomberg chats, Slack messages, WhatsApp messages, etc.) be archived. In 2023, the SEC initiated the "Off-Channel Communications" initiative and began assessing penalties against various institutions for the failure of those institutions to capture employee text messages. UK and EU regulators have also signalled that regulatory scrutiny will be placed on the same types of misconduct. If an insider claims to have received a trade pre-clearance or compliance advice via an "off-channel" unmonitored source of electronic communication, regulators will likely be very sceptical. As such, compliance departments should implement measures to restrict illicit channels of communication (i.e., personal WhatsApp) and provide archiving or monitoring tools to preserve the integrity of communications.

CONCLUSION

Insider Trading Regulations Globally: Regulators focus on ensuring that all trading communications get recorded; also, regulators require disclosures to be complete and specific. Former safe havens for companies were available, like benign 10b5-1 plans or delayed disclosures, but these have now been reduced significantly. Companies and managers will now need to convert their processes to include a robust pre-approval process, comprehensive recordkeeping, and up-to-date surveillance of digital communications.

Insight for Compliance Professionals: The technologies used by employees (i.e., smartphones, Slack apps, and unencrypted communications) now provide regulators with prima facie evidence. Essentially, every communications tool that you use today has become a recording device if corrupt individuals misuse it. As a result, compliance teams must consider all communications as possibly being discoverable.

Call to Action: All firms should conduct a gap analysis today to evaluate all pre-clearance and disclosure procedures and identify areas of weakness. In addition, firms should ensure that all personal trading activities involve both a supervisor and legal counsel in the loop before execution. The same message applies whether your company is in New York City, London, England, Mumbai, India, or any other worldwide location: document all MNPI activities; coordinate MNPI actions with others in the firm; and correspondingly disclose all trades made.

Proactive compliance not only prevents fines and bans from the market, but it also supports maintaining the trust of participants in the market.