GREENWICH COMPLIANCE

SPOTLIGHT ON

Insider Trading: §204A and Other Requirements

The contents of this Spotlight have been prepared for informational purposes only and should not be construed as legal or compliance advice.

Insider trading has been thoroughly discussed and debated elsewhere. The infamous violation arising out of Section 10(b) and Rule 10b-5 of the Exchange Act of 1934 is arguably the greatest nightmare of investment professionals. The classic theory (that involves corporate executives) and the misappropriation theory (that involves temporary insiders such as outside counsels, consultants, or accountants) have been aggressively utilized by the SEC and Department of Justice. Investment advisory firms that are neither actual nor temporary insiders could be liable for failure to maintain an adequate supervisory program or supervise their employees. This Spotlight focuses on the requirements under Section 204A of the Investment Advisers Act ("Advisers Act"), which is designed to bolster the insider trading prohibitions found elsewhere in the federal securities laws. This provision's coverage is broader than that of the Code of Ethics Rule, which applies to personal securities transactions by an adviser and its representatives.

Insider Trading Revisited

Insider trading generally occurs when a person trades securities while in possession of material, non-public information or improperly communicates that information to others ,such as tips from actual or temporary insiders. Information is considered "material" when there is a substantial likelihood that a reasonable investor would consider the information important in making an investment decision.[1] Information is considered "non-public" until it has been disseminated broadly to investors in the marketplace.

Traditional inside information includes information about an issuer that has not been broadly disseminated to the investing public like significant M&A plans, earnings estimates, changes, dividend changes, major litigation problems, pending bankruptcy, or a major labor dispute.[2] In the context of an investment advisory firm, information about a client's positions or trading plans and patterns would usually be considered inside information. Certain investment strategies such as distressed securities investing, merger arbitrage, or syndicated loans can also result in investment advisers obtaining inside information.[3]

Section 204A requires every investment adviser to establish, maintain, and enforce written policies and procedures reasonably designed, taking into consideration the nature of such

[1] See Basic v. Levinson, 485 U.S. 224 (1988) (A landmark case where the SCOTUS articulated the "fraud-on-the-market-theory.").
[2] Lemke and Lins, Regulation of Investment Advisers, §2:171, (2020ed).
[3] Id.

investment adviser's business, to prevent the misuse of material, non-public information by such investment adviser or any person associated with the investment adviser.

Recommended Procedures

Section 204A contemplates that potential sources of inside information and measures necessary to prevent the violation may vary among advisers depending on the services an adviser offers and its personnel's actvities.[4] The SEC has not issued any definitive guidelines on what measures are appropriate to comply with Section 204A. Therefore, an investment adviser's policies and procedures must be adapted to its business's unique nature. For instance, an adviser with a designated research analyst in charge of cultivating industry sources may need to adopt specific procedures to monitor the analyst's interactions with issuer contacts. Nevertheless, a number of basic, generally useful guidelines should be applicable to all advisers.[5] They are the following:

1. **Appoint a compliance officer** that oversees a firm's compliance program and gives guidance about inside information. For registered investment advisers and fund managers, a CCO is required by law.

2. **Written policies and procedures** should explain the ethical, business, and legal reasons for avoiding insider trading and instruct employees to direct questions and inquiries to the CCO. Further, employees with access to sensitive information should make attestations to reading and understanding these policies and procedures periodically.

3. **Develop a training program** that highlights the different types of conflicts of interest that may be present in particular situations as well as update employees as to recent developments or revised requirements.

4. **Adopt a Chinese Wall** – physical and organizational information barriers— in order to limit or contain the flow of material, non-public information to those with a "need to know.'' These information barriers may involve restricting access to information, separating certain functions—investment banking, proprietary trading or advisory services—into separate subsidiaries or departments, and establishing separate recordkeeping and support systems. Additionally, the SEC urges firms to maintain sufficient documentation to recreate actions taken pursuant to information barrier procedures, particularly analyses and investigations of employee and proprietary trading.[6]

5. **Review of employee trading** in connection with the Code of Ethics. Particularly, firms may require preclearance or reporting of all employee trading in securities in order to monitor

[4] O'Malley, Walsh and Watts, Investment Adviser's Legal and Compliance Guide §5.03 (3rd ed, 2020-2 supp).
[5] Lemke and Lins, Regulation of Investment Advisers, §2:171, (2020ed).
[6] See SEC Office of Compliance Inspections and Examinations, "Staff Summary Report on Examinations of Information Barriers: Broker-Dealer Practices under Section 15(g) of the Securities Exchange Act of 1934".

potential misuse of information. Firms should have procedures to review employee and proprietary trading on a periodic basis, specifying both the frequency and the reviewer. If an employee may have a brokerage account at another firm, there may be a requirement that duplicate confirmation and account statements be provided to the CCO at the employee's firm. Firms may also require that employees disclose any public companies of which the employee is an officer, director, or 10% shareholder. These would generally include reviewing of brokerage confirmations and account statements, comparing them to restricted and watch lists, and looking particularly for unusual transactions or trading patterns.

6. **Restricted Lists, Watch Lists, and Rumor Lists**. For firms that engage either directly or through affiliates in investment banking, research or trading, restricted lists and watch lists may be appropriate, depending on the firm's structure and organization:

    - Restricted lists set forth securities in which employee or proprietary transactions are prohibited or limited.
    - Watch lists set forth those securities in which trading is not per se prohibited but closely monitored. Watch lists are distributed only to a limited number of persons.
    - Rumor lists, while not an essential part of a Chinese Wall, are sometimes also maintained by firms and are encouraged by the SEC. A rumor list sets forth securities that become the subject of rumors, such as an impending third-party deal.

7. **Exception reports and investigations** should be maintained to record the details of any transaction by an employee or proprietary account in a security on a restricted list or watch list. A firm must investigate cases where proprietary or employee transactions occur in securities on a restricted or watch list or where material, non-public information may have been used.

8. **Controlling and securing confidential information** in locked physical or electronic files is a basic but effective way to keep such information from being misused. As a general practice, confidential information should be communicated only to those employees or persons with a "need to know" such information.

Enforcement Actions

The SEC has brought several enforcement proceedings against investment advisers for failing to establish and maintain the required policies and procedures or failing to adhere to them, sometimes where there was no collateral wrongdoing and no apparent misuse of material, non-public information.[7] Moreover, the Department of Justice has brought criminal proceedings against hedge fund managers, in both individual and corporate capacities, for insider trading.

[7] Lemke and Lins, Regulation of Investment Advisers, §2:171, (2020ed).

1. Steven Cohen and S.A.C. Capital Advisors, LP[8]

S.A.C. Capital Advisors, L.P. was once a $14-billion hedge fund empire with one of Wall Street's best records for performance. Steve A. Cohen, the owner, and namesake of SAC was crowned "the king of hedge funds" and a frequent subject of major media publications. In 2013, SAC was charged with one count of wire fraud and four counts of securities fraud in connection with alleged insider trading by numerous employees at various times over a decade. The DOJ's 41-page indictment detailed a culture that had encouraged trading based on inside information. Specifically, Mr. Cohen has tolerated, ignored, fostered, or otherwise allowed SAC's insider trading culture. Until 2008, SAAC had a policy of purging all IMs after thirty-six hours and all emails not specifically saved after thirty days. Although the compliance department had recommended reviewing electronic communications by employees, they were rarely reviewed. Furthermore, there was a trail of insider trading that surrounded SAC, which was evidence of the type of corporate culture fostered at SAC in which using questionable means to obtain an "edge" was commonplace. The history of SAC employees contained many who were accused and convicted of insider trading. It was difficult to find the records of internal audits on questionable trades at SAC, and sanctions against traders appeared to be non-existent.

Mr. Cohen personally and SAC were criminally charged with various counts of fraud, including securities fraud and mail/wire fraud, although Mr. Cohen had no actual knowledge of criminal activities committed by employees. Whether Mr. Cohen's lack of compliance oversight equals to scienter—a critical component of a securities fraud conviction—remains controversial among criminal law experts (Mr. Cohen did not plead guilty); however, in civil proceedings pursed by the SEC, Mr. Cohen and the firm's wholesale failure to implement effective compliance procedures was a blatant violation of Section 204A.

2. Merrill Lynch[9]

Merrill Lynch is a dually registered broker-dealer and investment adviser with the SEC. From 2002 to 2004, several Merrill Lynch retail brokers permitted day traders to hear confidential information regarding Merrill Lynch institutional customers' unexecuted orders as they were transmitted over Merrill Lynch's squawk box system. The equity squawk box was an industry-standard audio communication tool that Merrill Lynch's institutional equities business uses to allow position traders to transmit customer order information internally, among other

[8] See Chapman, Frances E.; Jennings, Marianne; and Tarasuk, Lauren "SAC Capital: Firm Criminal Liability, Civil Fines, And the Insulated CEO," American University Business Law Review, Vol. 4, No. 3 (2015). Available at: http://digitalcommons.wcl.american.edu/aublr/vol4/iss3/1; "Feds Charge SAC Capital Insider Trading Case", NPR, available at https://www.npr.org/sections/thetwo-way/2013/07/25/205445770/feds-charge-sac-advisors-with-insider-trading.

[9] *In the matter of Merrill Lynch, Pierce, Fenner, & Smith Inc*. Inv. Adv. Rel. No. 2851 (Mar. 11, 2009), available at https://www.sec.gov/litigation/admin/2009/34-59555.pdf.

information. The day traders used the customer order information to "trade ahead" of the institutional customer orders and, in many instances, profited from price movements that were caused by the market impact of the institutional customer order. The day traders compensated the brokers for access to this material, non-public order information through commissions and cash payments.

Merrill Lynch maintained policies prohibiting insider trading, the front running of customer orders, and the improper disclosure of customer order information. Merrill Lynch informed its brokers, including those brokers who improperly disclosed customer order information to day traders, of these policies. However, Merrill Lynch lacked written policies or procedures to limit access to the equity squawk box, track which employees had access to the equity squawk box or monitor employees' use of the equity squawk box. Consequently, an undetermined number of retail brokers received access to equity squawk boxes despite the absence of any bona fide need for the information, such as demonstrating any ability to fill block orders; Merrill Lynch was unable to identify which employees had equity squawk boxes; and several retail brokers were able to provide equity squawk box information to day traders simply by placing their telephone receiver next to the equity squawk box for the entire trading day.

Given Merrill Lynch's extensive financial businesses, certain categories of employees were regularly in possession of material, non-public information, or in contact with employees in possession of such information pertaining to Merrill customers and clients. Merrill Lynch failed to maintain written policies or procedures that reasonably: (a) limited access to the equity squawk box to those employees with a bona fide business need for the customer order information; (b) tracked who had access to the equity squawk box; or (c) instructed supervisors on how to control access to, or monitor the use of, the equity squawk box. Therefore, Merrill Lynch violated Section 204A.

3. Morgan Stanley[10]

Morgan Stanley is a dually registered broker-dealer and investment adviser with the SEC. Morgan Stanley had certain policies and procedures designed to prevent misuse of material non-public information. Among other things, Morgan Stanley maintained a "Watch List" of companies about whom Morgan Stanley was in possession of material non-public information. Due to a systemic breakdown in the critical compliance function, Morgan Stanley failed to conduct any surveillance of a massive number of accounts and securities. Morgan Stanley's specific failures included the following:

- From at least 2000 to 2004, Morgan Stanley failed to conduct any Watch List surveillance of hundreds of thousands of employee and employee-related accounts to determine

[10] *In re Morgan Stanley & Co.*, Inc., Inv. Adv. Act Rel. No. 2526 (June 27, 2006), available at https://www.sec.gov/litigation/admin/2006/34-54047.pdf.

whether securities in those accounts had been purchased or sold on the basis of material non-public information.

• From at least 1999 to 2003, Morgan Stanley failed to conduct any daily Watch List surveillance of trading in any accounts with respect to some or all of the securities of approximately 3,000 issuers that had been placed on the firm's Watch List specifically so that trading in those securities would be monitored.

• From as early as 1997 until as late as 2005, Morgan Stanley failed to conduct any surveillance of trading in approximately 900 employee accounts held outside of Morgan Stanley and approximately 30,000 employee accounts held at Morgan Stanley that the firm failed to identify as held by employees.

• From at least 2001 until 2004, Morgan Stanley failed to conduct any of the surveillance required by its policies of certain types of securities traded in MSDW and MS & Co. accounts, including certain derivative securities, single stock futures, and equity options pertaining to issuers that Morgan Stanley had placed on its Watch List.

Morgan Stanley was in violation of Section 204A because it failed to maintain and enforce written procedures reasonably designed, taking into consideration the nature of Morgan Stanley's business, to prevent misuse, in violation of the federal securities laws. Although Morgan Stanley had written policies requiring that it conduct surveillance of trading in Watch List securities, Morgan Stanley failed to maintain and enforce those policies to the extent that it failed to conduct any surveillance with respect to hundreds of thousands of employee and employee-related accounts during a multi-year.

Conclusion

The SEC has consistently made clear that investment advisers must take their responsibilities seriously to design and enforce sufficiently robust policies and procedures to prevent the misuse of material non-public information. Unlike a conviction of a Rule 10b-5 violation under the Exchange Act, Section 204A of the Advisers Act does not require a showing of scienter or actual trading in possession of material, non-public information. As a result, in many cases like those presented above, the SEC sanctioned advisers for inadequate insider trading procedures where there was no collateral wrongdoing and no apparent misuse of material, non-public information. When drafting insider trading policies and procedures, in addition to common measures laid out in this Spotlight, an adviser should consider the nature of their business services, outside positions held by firm employees, and other activities and the personal relationships of the firm's personnel.[11]

[11] O'Malley, Walsh and Watts, Investment Adviser's Legal and Compliance Guide §5.03 (3rd ed, 2020-2 supp).