Chapter 49

Investment Banking Compliance

Russell D. Sacks*

Partner, King & Spalding LLP

Steven R. Blau

Counsel, King & Spalding LLP

[Chapter 49 is current as of April 3, 2023.]

* The authors gratefully acknowledge the contributions to this chapter by Sumon Dantiki, Shaswat Das, Robert Dedman, Timothy Fesenmyer, Sean Kelly, James McMullin, and Andrew Michaelson, and to earlier versions of this chapter by Robert Evans III and Richard B. Alsop.

§ 49:1 Information Control

§ 49:1.1 Insider Trading

[A] Generally

Insider trading has traditionally been the most important compliance issue for persons involved in investment banking. Insider trading is the trading of a company's securities by persons in possession of material nonpublic information about the company. Insider trading can take place legally, such as when corporate insiders buy and sell securities in their own companies in compliance with the regulations governing such trading and their own internal company guidelines, and illegally, such as when corporate insiders with material nonpublic information use that information improperly for personal gain to make profits or avoid losses.[1]

1. Selective Disclosure and Insider Trading, Exchange Act Release No. 43,154, 2000 WL 1201556, at *24, n.125 (Aug. 15, 2000) [hereinafter Selective Disclosure and Insider Trading Release].

"Material information" has been defined by the U.S. Supreme Court as information where: (i) there is a "substantial likelihood" that a "reasonable investor" would consider the information important in making an investment decision; (ii) the disclosure of the information would be "viewed by the reasonable investor as having significantly altered the 'total mix' of information made available";[2] or (iii) the disclosure of the information is "reasonably certain to have a substantial effect on the market price of the security."[3]

The U.S. Securities and Exchange Commission (SEC) has described "nonpublic information" as information that has not been disseminated or made available to investors generally.[4]

Sources of inside information include corporate officers or employees, corporate clients, corporate borrowers, non-corporate entities, such as government agencies, principal investments, corporate insiders, institutional investors, and research.[5]

[B] Legal Framework

[B][1] Securities Exchange Act § 10(b)

Section 10(b) of the Securities Exchange Act of 1934 (the "Exchange Act") and Rule 10b-5 promulgated thereunder prohibit fraud in connection with the purchase or sale of securities. Courts have interpreted section 10(b) and Rule 10b-5 to prohibit the purchase or sale of securities on the basis of material nonpublic information in breach of a duty preventing the use of such information for personal gain.[6]

---

2. Basic Inc. v. Levinson, 485 U.S. 224, 231–32 (1988), quoting TSC Indus., Inc. v. Northway, Inc., 426 U.S. 438, 448–49 (1976).
3. Elkind v. Liggett & Myers, Inc., 635 F.2d 156, 166 (2d Cir. 1980), quoting TSC Indus., Inc. v. Northway, Inc., 426 U.S. 438, 449 (1976).
4. Selective Disclosure and Insider Trading Release, *supra* note 1.
5. 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 (Sept. 27, 2012) [hereinafter STAFF SUMMARY REPORT ON EXAMINATIONS OF INFORMATION BARRIERS].
6. In addition to liability arising from the classic case of insider trading, where a corporate insider trades in securities on the basis of material nonpublic information, liability under Rule 10b-5 can arise when information has been misappropriated. Misappropriation occurs when an outsider trades in violation of a duty of confidentiality and loyalty owed to someone else. *See* United States v. O'Hagan, 521 U.S. 642 (1997); Chiarella v. United States, 445 U.S. 222 (1980). Rule 10b5-2 "provides a non-exclusive definition of circumstances in which a person has a duty of trust or confidence for purposes of the 'misappropriation' theory of insider trading." 17 C.F.R. § 240.10b5-2 (2000). In United States v.

Rule 10b5-1, promulgated in 2000, provides affirmative defenses to violations of Rule 10b-5, including a provision that a broker-dealer or other entity may "demonstrate that a purchase or sale of securities is not 'on the basis of' material nonpublic information" if the person making the investment decision was not aware of the information, and the broker-dealer or other entity had implemented reasonable policies and procedures to ensure that investment decisions would not be based on such information.[7] In the release accompanying the rule, the SEC noted that a broker-dealer could reduce the risk of trading desk awareness of material nonpublic information by "segregat[ing] its personnel and otherwise us[ing] information barriers so that the trader for the firm's proprietary account is not made aware of the material nonpublic information."[8]

[B][2] Insider Trading and Securities Fraud Enforcement Act

In the 1984 Insider Trading Sanctions Act (ITSA), Congress gave the SEC more power to combat insider trading.[9] In 1988, amid

---

Newman, 773 F.3d 438 (2d Cir. 2014), the Second Circuit declined to accept the theory that a defendant who receives information indirectly—a so-called "remote tippee"—need not know that the insider had disclosed material nonpublic information in exchange for a personal benefit (while the government petitioned for *certiorari* with respect to certain aspects of this decision, it did not do so on the question of whether a remote tippee has to know about the benefit conferred on the insider; the Supreme Court rejected the petition in any event). Because industry participants frequently receive information indirectly, the *Newman* decision has caused some institutions to consider whether their policies should define insider trading more narrowly such that trading is prohibited only when the recipient of information knows that it was disclosed in breach of duty *and* in exchange for a benefit. In fact, however, the *Newman* decision's application in the context of investment banking compliance has thus far been limited because investment banking compliance has traditionally ignored the question of whether the insider received a benefit. More recently, the Second Circuit affirmed that *Newman*'s "meaningfully close personal relationship" test is still valid for determining whether an insider tipper received a personal benefit (and thus breached a fiduciary duty), but also held that the test will be satisfied upon a showing that (1) the "tipper and tippee shared a relationship suggesting a quid pro quo" or (2) "the tipper gifted confidential information with the intention to benefit the tippee." United States v. Martoma, 894 F.3d 64 (2d Cir. 2018).

7. 17 C.F.R. § 240.10b5-1(c)(2) (2000).
8. Selective Disclosure and Insider Trading Release, *supra* note 1, at *24, n.125.
9. Insider Trading Sanctions Act of 1984, Pub. L. No. 98-376, § 2; 98 Stat. 1264 (1984).

several insider trading scandals, Congress passed the Insider Trading and Securities Fraud Enforcement Act (ITSFEA).[10] Congress intended the act to "augment enforcement of the securities laws, particularly in the area of insider trading, through a variety of measures designed to provide greater deterrence, detection and punishment of violations . . . ."[11]

ITSFEA created section 15(f) of the Exchange Act, renumbered as section 15(g) by the Dodd-Frank Wall Street Reform and Consumer Protection Act (the "Dodd-Frank Act"),[12] which, for the first time, created an affirmative duty for broker-dealers to "establish, maintain and enforce written policies and procedures reasonably designed . . . to prevent the misuse . . . of material nonpublic information."[13]

Section 15(g) requires broker-dealers not only to implement information barriers to prevent the misuse of material nonpublic information, but also to regularly review and to vigorously enforce the barriers. ITSFEA expanded the enforcement power of the SEC by allowing it to seek sanctions against firms that fail to have adequate policies and procedures in place, even if no actual trading violations occur.[14] ITSFEA does not expressly outline the types of procedures necessary to avoid liability; however, the ITSFEA House Report cited some examples, including:

- restraining access to files likely to contain material nonpublic information;
- providing continuing education programs concerning insider trading regulations;
- restricting or monitoring trading in securities about which firm employees possess material nonpublic information; and
- diligently monitoring trading for firm or individual accounts.[15]

---

10. Insider Trading and Securities Fraud Enforcement Act of 1988, Pub. L. No. 100-704, 102 Stat. 4677 (1988).
11. H.R. REP. NO. 100-910, at 7 (1988), *reprinted in* 1988 U.S.C.C.A.N. 6043, 6044 [hereinafter ITSFEA House Report].
12. Pub. L. No. 111-203, 124 Stat. 1376 (2010).
13. Securities Exchange Act of 1934, 15 U.S.C. § 78o(f) (section 15(g)).
14. For an example of a case in which the SEC brought charges under section 15(g) without identifying trading violations, see Litigation Release No. 20,551 (May 1, 2008) (announcing the filing and settlement of a civil complaint against Chanin Capital LLC for failure to establish, maintain, and enforce adequate procedures under section 15(g)).
15. ITSFEA House Report, *supra* note 11, at 22 (reprinted in 1988 U.S.C.C.A.N. 6043, 6059).

Following the passage of ITSFEA, the SEC Division of Market Regulation (the "Division") published a report in March 1990 of its review and analysis of broker-dealers' information barrier policies and procedures.[16] Although ITSFEA explicitly granted the SEC broad powers to mandate specific policies to be adopted by broker-dealers, the SEC provided some general observations regarding the elements of an adequate information barrier and concluded that the self-regulatory organizations (SROs)[17] were best equipped to test the adequacy of current broker-dealer policies and procedures and to formulate any required improvements or modifications.[18] Throughout its report, the Division emphasized the need to tailor a firm's policies and procedures to the nature of its businesses and the importance of a firm's compliance department to the proper functioning of the firm's information barriers. In June 1991, the NASD and the NYSE issued a Joint Memo on Chinese Wall Policies and Procedures, discussing the minimum elements necessary to create and maintain an adequate information barrier.[19]

§ 49:1.2 *Information Barriers*

[A] Generally

Multi-service firms establish information barriers[20] to restrict the flow of material nonpublic information between employees who

16. *See* Broker-Dealer Policies and Procedures Designed to Segment the Flow and Prevent the Misuse of Material Non-Public Information, Fed. Sec. L. Rep. ¶ 84,520 (Mar. 1, 1990) [hereinafter 1990 SEC Market Reg. Report].
17. FINRA was formed in 2007 upon the merger of the NASD and certain divisions of the NYSE. The FINRA rulebook currently consists of both NASD rules and certain NYSE rules that FINRA has incorporated. For purposes of this outline, these rules will be referred to as NASD and NYSE rules, respectively, or where applicable FINRA rules. FINRA also has incorporated certain interpretive guidance issued by the NASD and the NYSE related to NASD rules and the incorporated NYSE rules. *See* Order Approving Proposed Rule Change to Amend the By-Laws of NASD to Implement Governance and Related Changes to Accommodate the Consolidation of the Member Firm Regulatory Functions of NASD and NYSE Regulation, Inc., SEC Release No. 34-56145 (July 26, 2007), https://www.sec.gov/rules/sro/nasd/2007/34-56145.pdf.
18. *See* 1990 SEC Market Reg. Report, *supra* note 16.
19. NASD/NYSE Joint Memo on Chinese Wall Policies and Procedures, NASD Notice to Members 91-45 (June 21, 1991), NYSE Information Memo 91-22 (June 28, 1991) ("NASD/NYSE Joint Memo").
20. The legislative history of ITSA reveals strong support for the idea that effective information barriers can provide a defense to alleged insider trading violations. The then-Chairman of the SEC stated in a letter to

regularly receive or develop that type of information, such as investment bankers, and employees who buy, sell, or recommend the securities to which the information relates.[21] Information barrier policies and procedures initially adopted by firms generally focused primarily on the control of material nonpublic information obtained by investment bankers in connection with corporate transaction and advisory assignments. However, there are other potential sources of material nonpublic information that require careful handling.[22] While the nature of investment banking activities has led regulators and investment banks themselves to focus on material nonpublic information, it is worth mentioning that regulators' and investment banks' focuses have increasingly evolved to consider protection and control of all confidential information, even if the same does not constitute material nonpublic information about a public company. This is because, increasingly, poor control of confidential information, broadly defined, is perceived to lead to violations of other regulations (for example, privacy), or to poor customer experience for investment banking customers.

[B] Effective Information Barriers: Minimum Elements

Firms have flexibility to tailor information barriers, but the SEC and SROs have set certain minimum elements of an effective information barrier program.

Congress that "[I]t is . . . important to recognize that, under both existing law and the bill, a multiservice firm with an effective Chinese wall [or information barrier] would not be liable for trades effected on one side of the wall, notwithstanding inside information possessed by firm employees on the other side." Letter from John S. R. Shad to Rep. Timothy E. Wirth (June 29, 1983), *reprinted in* H.R. REP. NO. 98-355, at 28 n.52 (1983) (the "1984 Act Report"), *reprinted in* 1984 U.S.C.C.A.N. 2274, 2301 n.52.

21. There is a distinction to be noted between public-side versus private-side business groups. Public-side groups do not have access to material nonpublic information on a routine basis. On the other hand, private-side groups are areas that have routine or ongoing access to material nonpublic information and, typically, it is assumed that people in these groups do have material nonpublic information. Groups such as: Investment Banking, Credit, Capital Markets, Syndicate, and support and control groups of these areas are considered to be private-side. *See* STAFF SUMMARY REPORT ON EXAMINATIONS OF INFORMATION BARRIERS, *supra* note 5, at pt. IV.

22. For example, research departments' knowledge of to-be-published research reports is considered to be material nonpublic information.

[B][1] Written Policies and Procedures

Information barrier policies and procedures must be incorporated in a firm's procedure and policy manuals and must restrict material nonpublic information to employees who have a "need to know" such information. These procedures include: policy statements, restrictions on access to records and support systems for sensitive departments, and supervision of all interdepartmental communications ("wall-crossing") involving material nonpublic information. There is leeway to compartmentalize organizations within the firm (such as between the investment banking business and the sales/trading/research businesses), but it is still important to incorporate a "need to know" policy within organizations. Information can be subject to non-disclosure requirements even if it is confidential, but not material. As a result, some firms have imposed the "need to know" policy more broadly to apply to all types of confidential information.

[B][2] Wall-Crossing Procedures

Firms must have "wall-crossing" procedures designed to facilitate situations that require an employee to cross an information barrier. Wall-crossings must be controlled and monitored, preferably by the compliance departments, must be specifically documented in writing and records must be retained.

[B][3] Restricted List and Watch List

The restricted list is a list of issuers whose securities or other financial instruments are subject to restrictions on sales, trading, or research activity. An issuer or security may be placed on the restricted list in order to reinforce a firm's information barrier, to comply with trading practices and other rules, to avoid the potential appearance of impropriety, or to meet other compliance or regulatory objectives. When an issuer appears on the restricted list, certain sales, trading and research activities involving that issuer's securities or other financial instruments may be restricted. Restricted activities may include: proprietary trading, including market-making; solicitation of client orders; the recommendation of the issuer's securities; and transactions for any employee or related account with respect to the related securities or financial instruments. The restricted list is usually maintained by a firm's compliance department, or by an institutional control room.

The watch list (sometimes called the "grey list") is a confidential list of issuers or securities about which a firm may have received or may expect to receive material nonpublic information, or about which the firm expects a reason to monitor activities. The placement of an issuer or security on the watch list generally will not affect sales

and trading activities, except by personnel who have access to material nonpublic information that may be the reason for the addition to the watch list. Trading in and research regarding watch-list securities or issuers are subject to surveillance by the firm's compliance department. The contents of the watch list and any related restrictions that may be imposed by the legal or compliance department are extremely confidential, and access to the watch list is very limited.

Firms that conduct both investment banking and research or arbitrage activities must maintain some combination of restricted and watch lists, and should conduct regular reviews of trading in securities appearing on the lists.[23] The SROs set forth specific minimum documentation standards concerning such lists, including records of the firm's methods for conducting reviews of employee and proprietary trading, the firm's procedures for determining whether trading restrictions will be implemented and the firm's explanations of why, when, and how a security is placed on or deleted from a restricted or watch list.[24] Further, the firm must adequately document how it monitors employee trading outside the firm of securities on the restricted or watch lists.

[B][4] Surveillance of Trading Activity

Firms must take reasonable steps to investigate any possible misuse of material nonpublic information, including any transactions in restricted or watch-list securities. Each investigation initiated must be documented and should include the name of the security, the date the investigation began, an identification of the accounts involved, and a summary of the disposition of the investigation.

[B][5] Physical and Electronic Separation

Information barriers must include arrangements for reasonable physical separation of public-side businesses (for example, sales and trading) from private-side businesses (for example, investment banking) that regularly receive confidential information. Information

---

23. Even firms that do not conduct investment banking, research, or arbitrage activities must have documented procedures to review employee and proprietary trading for misuse of material nonpublic information. *See* 1990 SEC Market Reg. Report, *supra* note 16, at pt. III.

24. The NASD/NYSE Joint Memo further mandates documentation for the use of restricted lists and watch lists. First, the firm must develop reasonable written standards or criteria for placing a security on and deleting a security from such lists. Second, documentation must include the date and, for restricted lists, the time the security was added to or deleted from the list.