Financial Fraud Law Report

AN A.S. PRATT & SONS PUBLICATION OCTOBER 2014

LexisNexis

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call:

Catherine Dillon at 908-673-1531
Email: ..... catherine.dillon@lexisnexis.com

For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at . . . . . (800) 833-9844
Outside the United States and Canada, please call . . . . . (518) 487-3000
Fax Number . . . . . (518) 487-3584
Customer Service Web site . . . . . http://www.lexisnexis.com/custserv/

For information on other Matthew Bender publications, please call

Your account manager or . . . . . (800) 223-1940
Outside the United States and Canada, please call . . . . . (518) 487-3000

Library of Congress Card Number: 80-68780

ISBN: 978-0-7698-7816-4 (print)
ISBN: 978-0-7698-7958-1 (eBook)

Cite this publication as:

Financial Fraud Law Report § [sec. no.] (LexisNexis A.S. Pratt);
Financial Fraud Law Report § 1.01 (LexisNexis A.S. Pratt)

Because the section you are citing may be revised in a later release, you may wish to photocopy or print out the section for convenient future reference.

An A.S. Pratt™ Publication

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2014–Pub.4759)

Editor-in-Chief & Board of Editors

POSTMASTER: Send address changes to the *Financial Fraud Law Report*, LexisNexis Matthew Bender, 121 Chanlon Road, North Building, New Providence, NJ 07974. Direct inquiries for editorial department to catherine. dillon@lexisnexis.com. *ISBN: 978-0-76987-816-4*

Insider Trading – Broker-Dealer Compliance Requirements and Best Practices

Daniel A. Nathan, Michael R. Sorrell, and Kali Schellenberg*

This article explores the current state of regulation and recent precedent regarding the role of broker-dealers in preventing and detecting insider trading, and offers guidance on how firms can avoid liability in this area.

Introduction

The focus is back on insider trading, and broker-dealers should be prepared. Regulatory bodies, particularly the Securities and Exchange Commission ("SEC") and the Financial Industry Regulatory Authority ("FINRA"), are combatting insider trading on many fronts, including the enforcement of requirements that broker-dealers implement procedures for preventing and detecting insider trading.[1] In its 2013 Examination Priorities Letter, FINRA emphasized insider trading as a top regulatory priority, and offered guidance underscoring the fact that, while individual bad actors are a clear target, broker-dealers that house these actors, or whose procedures leave open a gap—however small—allowing for potential insider trading to occur or go unnoticed, may find themselves facing a costly regulatory action. This article explores the current state of regulation and recent precedent regarding the role of broker-dealers in preventing and detecting insider trading, and offers guidance on how firms can avoid liability in this area.

---

* Daniel A. Nathan (dnathan@mofo.com) is a partner at Morrison & Foerster LLP in the firm's Securities Litigation, Enforcement and White-Collar Defense Group. Michael R. Sorrell (msorrell@mofo.com) is an associate at the firm. Kali Schellenberg was a summer associate at the firm.

[1] While this article focuses on the SEC and FINRA, firms have also been subject to vigorous enforcement by other government agencies and regulators. For example, while in the context of hedge funds, the government's prosecution of SAC for insider trading touches on a broker-dealers' responsibilities to prevent insider trading and maintain a healthy firm culture. *See* Patricia Hurtado, *SAC Record $1.8 Billion Insider Plea Caps 7-Year Probe*, Bloomberg (Apr. 10, 2014), http://www.bloomberg.com/news/2014-04-10/sac-judge-approves-record-insider trading-accord-with-u-s.html. There have also been numerous state-level actions against firms for conduct outside of traditional insider trading, such as the selected disclosure of market-moving information or the premature distribution of research reports to certain clients. The New York Attorney General, Eric Schniederman, has dubbed these kinds of actions "Insider Trading 2.0," and vowed to crack down on them. Rachel Abrams, *Attorney General Vows to Crack Down on 'Insider Trading 2.0'*, The New York Times (Jan. 9, 2014), http://dealbook.nytimes.com/2014/01/09/attorney-general-vows-to-crack-down-on-insider-trading-2-0/.

FINRA and SEC Insider Trading Regulations

The SEC and FINRA enforce rules that cover a broad spectrum of activity related to insider trading. The foundation of SEC and FINRA enforcement in this area is the prohibition on insider trading under Section 10(b) of the Securities Exchange Act of 1934 ("Exchange Act") and SEC Rule 10b-5. When procedures designed to prevent insider trading are not in place, followed, or documented, broker-dealers may face an action by either regulator.

SEC

The SEC has actively brought actions against broker-dealers and their registered representatives and associated persons based on their mishandling of material, nonpublic information ("MNPI") under Exchange Act Section 15(g). Section 15(g)[2] requires every registered broker-dealer to "establish, maintain, and enforce written policies and procedures reasonably designed, taking into consideration the nature of such broker's or dealer's business, to prevent the misuse . . . of [MNPI]." If broker-dealers are dually registered as investment advisers, or closely integrated with an affiliated investment advisor, they may also be subject to liability under Section 204A of the Investment Advisers Act of 1940 ("Adviser's Act") and Rule 204A-1, promulgated thereunder, which have analogous requirements to Section 15(g).

If insider trading has occurred in violation of Exchange Act Section 10(b) and SEC Rule 10b-5, the SEC can also bring an action pursuant to Exchange Act Section 15(b)(4)(e) and (b)(6), or its counterpart, Section 203(e)(6) and (f) of the Adviser's Act, for failure to reasonably supervise with a view to preventing this violation.[3] In addition, even if no insider trading is proven to have taken place, the filing of suspicious activity reports ("SARs") pursuant to the Bank Secrecy Act is a mechanism for regulatory agencies to monitor insider trading,

---

[2] There is no requirement under Section 15(g) that there be an underlying insider trading violation or any other violation of the Exchange Act or the rules thereunder. *See In the Matter of New York Stock Exchange LLC, NYSE Arca, Inc., NYSE MKT LLC f/k/a NYSE Amex LLC, and Archipelago Securities, L.L.C*, Admin. Proceeding No. 3-15860, 2014 SEC LEXIS 1526 (May 1, 2014), *available at* http://www.sec.gov/litigation/admin/2014/34-72065.pdf.

[3] The SEC is currently pursuing an administrative proceeding under Advisers Act Section 203(f) against Steven A. Cohen, founder and owner of the hedge fund SAC, for failure to supervise with a view to preventing his employees' violations of Section 10(b) and Rule 10b-5. This action comes after two traders at SAC were convicted of insider trading and two others were sued but settled with the SEC. While SAC is a hedge fund, this action illustrates that those associated with firms can be personally prosecuted for failure to supervise when members of their organization participate in insider trading that allegedly should have been caught. *See In the Matter of Steven A. Cohen*, Admin. Proceeding No. 3-15382, 2013 SEC LEXIS 2119 (July 19, 2013), *available at* http://www.sec.gov/litigation/admin/2013/ia-3634.pdf.

and therefore broker-dealers may be subject to Exchange Act Section 17(a) and Rule 17a-8 thereunder if it is determined that they willfully filed inaccurate or misleading SARs. It is worth noting that in filing SARs, broker-dealers have a responsibility to report not only any potential misconduct by their employees, but also suspected illegal activity, including attempted insider trading, by their customers.[4]

Regulation FD[5] and Exchange Act Section 13(a) prohibit public companies from selectively disclosing MNPI to certain parties when it is foreseeable that those parties will trade on the information before it is available to the public. While this particular issue is outside the scope of most broker-dealer activity, it serves as a reminder to firms to pay close attention to their representatives, who may be making use of social media on a regular basis. The SEC recently connected the use of social media and insider trading when it issued a report that examined whether a public company and its CEO violated Regulation FD and Section 13(a) when the CEO used his personal Facebook account to make an announcement about the company.[6]

FINRA

FINRA enforces a variety of rules relating to insider trading against broker-dealers. As an initial matter, any violation of FINRA and National Association of Securities Dealers ("NASD")[7] rules as well as the federal securities laws is a violation of FINRA Rule 2010, which mandates "high standards of commercial honor and just and equitable principles of trade" for broker-dealers.[8] Certain rule violations may also implicate FINRA Rule 2020, which states that "[n]o member shall effect any transaction in, or induce the purchase or sale of, any security by means of any manipulative, deceptive or

---

[4] *See* FINRA, *FINRA Dispute Resolution Arbitrator Training: Anti-Money Laundering Requirements and Suspicious Activity Reporting*, at 13 (Aug. 2011), *available at* http://www.finra.org/web/groups/arbitrationmediation/@arbmed/@arbtors/documents/arbmed/p124130.pdf.

[5] 29 C.F.R. § 243.100 *et seq*.

[6] Securities and Exchange Commission, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: Netflix, Inc., and Reed Hastings*, Release No. 69279 (Apr. 2, 2013), *available at* http://www.sec.gov/litigation/investreport/34-69279.pdf.

[7] As the successor entity to the NASD, FINRA enforces legacy NASD rules that have not yet been incorporated into the FINRA rulebook.

[8] U.S.-registered brokers can be disciplined by FINRA under Rule 2010 based on violations of other, non-FINRA laws, including foreign laws. *See In the Matter of Kenneth Ronald Allen*, AWC 2012033432301 (June 30, 2014), *available at* http://disciplinaryactions.finra.org/viewDocument.aspx?DocNb=36603 (finding former equity trader violated FINRA Rule 2010 for selling short Japanese stock on the Tokyo Stock Exchange on the basis of inside information, in violation of Japanese securities laws).

other fraudulent device or contrivance." Areas that FINRA has identified as potentially implicating insider trading are anti-money laundering policies, governed under FINRA Rule 3310; the reporting of positional data, governed under FINRA Rule 2360(b)(5); and blue sheet data reporting, governed under Exchange Act Section 17(a), SEC Rules 17a-4 and 17a-25, and FINRA Rules 8211 and 8213. FINRA also enforces Rule 5270, which relates to insider trading in prohibiting front-running of block transactions. The rule essentially serves to prohibit broker-dealers from taking advantage of knowledge about an upcoming client block transaction by trading in the firm's own account.

Broker-dealers are also expected to establish and maintain systems and procedures designed to comply with rules aimed at preventing individual traders from engaging in insider trading. NASD Rule 3050, for example, requires disclosure of outside brokerage accounts. When a broker-dealer fails to establish, implement, or enforce internal policies and procedures to prevent and remediate violations of its rules, FINRA may also allege failure to supervise under FINRA Rule 3110 (formerly known as NASD Rule 3010).[9]

Recent Enforcement Actions Related to Insider Trading Procedures

The SEC and FINRA have identified insider trading as a top regulatory priority.[10] In recent years, against the backdrop of high-profile criminal and civil insider trading actions brought by the Department of Justice and the SEC, both FINRA and the SEC have initiated enforcement proceedings against, and entered into consent agreements with, broker-dealers that allegedly failed to meet their obligations under the regulatory regime. These proceedings and settlements reflect increased vigilance on the part of both agencies to ensure that firms are actively working to prevent and detect insider trading.

In recent SEC and FINRA enforcement actions, the agencies have concentrated on certain violations, including: 1) procedural failings related to insider trading prevention; 2) deficiencies in anti-money laundering policies; and 3) failures related to reporting requirements. Firms should consider enhancing compliance efforts in all three areas.

---

[9] FINRA and NASD rules have been updated and renumbered in recent years, with the next revision scheduled to take effect in December 2014.

[10] *FINRA 2014 Examination Priorities Letter*, at 7 (Jan. 2014), *available at* http://www.finra.org/web/groups/industry/@ip/@reg/@guide/documents/industry/p419710.pdf; *FINRA 2013 Examination Priorities Letter*, at 5 (Jan. 2013), *available at* http://www.finra.org/web/groups/industry/@ip/@reg/@guide/documents/industry/p197649.pdf; U.S. Securities and Exchange Commission, *Insider Trading*, https://www.sec.gov/answers/insider.htm ("Because insider trading undermines investor confidence in the fairness and integrity of the securities markets, the SEC has treated the detection and prosecution of insider trading violations as one of its enforcement priorities.").

Insider Trading Compliance Policies

The SEC and FINRA target the failures of broker-dealers to establish, implement, and/or enforce adequate insider trading compliance policies. An essential aspect of adequate insider trading policies is safeguarding MNPI. This is reflected clearly in SEC enforcement actions. In a May 2014 settlement, the SEC found that a broker-dealer violated Section 15(g) for not having electronic controls over non-displayed liquidity information when engaged in error trading.[11] In that case, the broker-dealer had no written policies or procedures about accessing this information, nor a system in place to prevent or monitor such access, which allowed personnel to anticipate possible shifts in a security's price from pending non-displayed orders.

While any procedural deficiency, such as the one discussed above, can trigger scrutiny, problems seemed to more commonly arise when broker-dealers developed new programs and services that raised new risks that were unaccounted for in their policies. For example, the SEC charged a broker-dealer under Section 15(g) after it had instituted a weekly "huddle program" but failed to update its supervisory procedures accordingly. In these huddles, research analysts, traders, and sometimes sales personnel met to discuss trading ideas, which were then shared with select clients. However, despite the risk that analysts could share MNPI about upcoming changes to their published research, the broker-dealer did not update its procedures and policies to combat these risks by, for instance, increasing surveillance over trading activity. A focal point of concern in the case was adequate monitoring of research analysts who were being increasingly utilized in the firm.

A similar issue arose in a 2011 SEC action against a broker-dealer under Section 15(g).[12] In that action, the broker-dealer began using research analysts' expertise to help investment bankers explore new business opportunities without revising its manual to take into consideration the analysts' new role. This oversight was part of the firm's larger failure to have a complete equity capital markets manual governing a portion of its business. Due in part to this mistake, employees did not understand their responsibilities; the firm's watch list was not adequately monitored; and the firewall between groups was not

---

[11] *In the Matter of New York Stock Exchange LLC, NYSE Arca, Inc., NYSE MKT LLC f/k/a NYSE Amex LLC, and Archipelago Securities, L.L.C*, Admin. Proceeding No. 3-15860, 2014 SEC LEXIS 1526 (May 1, 2014), *available at* http://www.sec.gov/litigation/admin/2014/34-72065.pdf.

[12] *In the Matter of Janney Montgomery Scott LLC*, Admin. Proceeding No. 3-14459, 2011 SEC LEXIS 3166 (July 11, 2011), *available at* http://www.sec.gov/litigation/admin/2011/34-64855.pdf.

effectively maintained. These errors, particularly the failure to review the firm's watch list, could allow for evidence of potential insider trading to go unnoticed.[13]

Failures related to newly-instituted policies were also at issue in at least four FINRA enforcement proceedings in the past two years. For example, FINRA settled formal disciplinary proceeding against a broker-dealer through a "Letter of Acceptance, Waiver and Consent" ("AWC") after the broker-dealer changed its business model without implementing new rules and procedures until over a year after the change.[14] Even though the company was in the process of revising its policies, FINRA found that the interim system was not adequately tailored to its business model. As a result, among other issues, reviews of employee trading activity—which can reveal potential insider dealing—were not performed according to the guidelines that were in place. In another action, FINRA accepted an AWC with a broker-dealer that opened a new branch office but failed to update its supervisory procedures such that the risks associated with that branch's work were not adequately combated.[15] Among the violations FINRA found in that case was the failure to identify a person responsible for insider trading compliance monitoring and the failure to document how and when such monitoring occurred.

Finally, simply having policies and procedures designed to prevent the abuse of MNPI will not insulate broker-dealers from liability. Broker-dealers must effectively implement and enforce policies and procedures, including documenting the same. Unsurprisingly, when an employee of a broker-dealer engages in insider trading, the SEC and FINRA scrutinize not only the firm's policies and procedures, but also its implementation and enforcement of such policies and procedures. If either is deemed inadequate, the firm – and not just

---

[13] Similar issues arose in *In the Matter of Monness, Crespi, Hardt & Co., Inc.*, No. 3-16025 (Aug. 20, 2014) (Order Instituting Administrative Cease-and-Desist Proceedings). The SEC alleged that the broker-dealer failed to comply with its policy that required the firm to add any issuer that was the subject of an upcoming research report to its restricted watch list, which would forbid personnel that might be privy to MNPI or the company from trading in the issuer's securities. The SEC further alleged that the company lacked compliance policies governing new company initiatives that brought together corporate management teams and investors through road shows and company personnel and investors through dinners. The company agreed to pay $150,000 to settle the SEC's claims.

[14] *In the Matter of KeyBanc Capital Markets, Inc.*, AWC 20090185906 (May 16, 2012), *available at* http://disciplinaryactions.finra.org/viewdocument.aspx?DocNB=31771.

[15] *In the Matter of Range Global LLC f/k/a Blue Trading, LLC and Navpoint, LLC*, AWC 20080160618 (Mar. 12, 2013), *available at* http://disciplinaryactions.finra.org/viewdocument.aspx?DocNB=33201.

the individual offender – may face significant penalties. Both the SEC and FINRA have penalized firms for failing to identify and prevent insider trading by individual employees, including the failures to commit adequate resources to its compliance program, to provide sufficiently specific procedures for implementation of the program, to assign responsibility for the program, and to ensure that reviews will be escalated when appropriate.

Anti-Money Laundering Procedures

Anti-money laundering ("AML") procedures help to identify and prevent insider trading violations. Several broker-dealers have been the subject of regulatory action for allegedly deficient AML policies, in particular for the failure to adequately tailor their procedures to their business model.[16] This failure was especially common amongst firms that traded in penny stocks, which FINRA has stated heighten the risk that suspect activity slips through the cracks. In a 2014 case, FINRA entered into an AWC with a broker-dealer after its AML policy allegedly did not allow for sufficient monitoring of trading. The settlement found that the firm was aware of suspicious activity, including possible insider trading by clients, yet did not make changes to prevent these occurrences.[17] The AWC also stated that the firm did not conduct satisfactory AML testing, as internal reviews failed to uncover shortcomings, address the firm's penny stock activity, or review recently-established surveillance systems.

In another action, in 2012, FINRA faulted a broker-dealer for failing to update its AML policies to reflect the nature of its business.[18] The firm was operating as an online broker-dealer trading in penny stock shares, which FINRA found exposed it to the risk that customers could use its platform to facilitate insider trading. The firm's AML procedures did not address this risk, and as a result the company did not adequately detect possible suspicious transactions, resulting in improperly filed SARs—a common allegation for broker-dealers whose AML policies are found to be insufficient. The SEC has also been active in this area, bringing an action in 2014 against a broker-dealer

---

[16] In a NASD notice to members issued in 2002, broker-dealers were instructed to ensure their AML procedures were tailored to their business model. Special NASD Notice to Members 02-21 (Apr. 2002), *available at* https://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p003704.pdf.

[17] *In the Matter of Brown Brothers Harriman & Co., Harold A. Crawford*, AWC 2013035821401 (Feb. 2, 2014), *available at* http://disciplinaryactions.finra.org/viewdocument.aspx?DocNB=35225.

[18] *In the Matter of Giovanni Ferrara*, Disciplinary Proceeding No. 20090166407-01 (July 30, 2012), *available at* http://disciplinaryactions.finra.org/viewDocument.aspx?DocNb=32134.

that included a charge for failing to file SARs pursuant to AML requirements under Exchange Act Rule 17a-8.[19]

Reporting Requirements

FINRA has also brought formal disciplinary proceedings against multiple broker-dealers for failures to comply with reporting requirements that could implicate insider trading. For example, FINRA brought at least three actions from 2013 to 2014 for the failure to correctly report conventional options positions to the Large Options Position Reporting ("LOPR") system. FINRA fined the three organizations $675,000, $750,000, and $1.15 million, respectively.

FINRA and the SEC also recently brought several actions against broker-dealers for inadequate blue sheet reporting, which is used by regulators to identify potentially violative trading. On June 4, 2014, FINRA entered into three AWC agreements and filed one complaint against broker-dealers who did not report blue sheet data correctly for various reasons—ranging from mathematical errors[20] to inaccurately reporting certain short-sale transactions as long-sale transactions.[21] In January 2014, the SEC settled an action against a broker-dealer whose blue sheet reports failed to report error account trades.[22] In all five matters, the regulators found that the firms' audit systems failed to provide accountability on the blue sheets, and, in one,[23] FINRA found that the supervisory system was not reasonably designed to achieve compliance with the law in accordance with NASD Rule 3010.

Best Practices to Avoid Liability

The SEC's "Staff Summary Report on Examinations of Information Barriers: Broker-Dealer Practices Under Section 15(g) of the Securities Exchange Act of 1934," issued in 2012, and FINRA's 2013 Examination Priorities Letter, provide instructive guidance on best practices for broker-dealers to avoid

---

[19] *In the Matter of Giovanni Ferrara, Disciplinary Proceeding* No. 20090166407-01, 6-7 (July 30, 2012), *available at* http://disciplinaryactions.finra.org/viewDocument.aspx?DocNb=32134.

[20] *In the Matter of FOLIO Investments, Inc.*, AWC 2013037231101 (June 4, 2014), *available at* http://disciplinaryactions.finra.org/viewdocument.aspx?DocNB=36215.

[21] *In the Matter of Goldman, Sachs & Co.*, AWC 2013037230001 (June 4, 2014), *available at* http://disciplinaryactions.finra.org/viewDocument.aspx?DocNb=36214.

[22] *In the Matter of Scottrade, Inc.*, Admin. Proceeding No. 3-15702, 2014 SEC LEXIS 373 (Jan. 29, 2014), *available at* http://www.sec.gov/litigation/admin/2014/34-71435.pdf.

[23] *Dept. of Enforcement v. Wedbush Securities Inc.*, Disciplinary Proceeding No. 2012034934301 (June 4, 2014), *available at* http://disciplinaryactions.finra.org/viewdocument.aspx?DocNB=36210.

liability.[24] The discussion below summarizes the risk controls highlighted by both agencies, together with added guidance gleaned from recent enforcement actions.

General Broker-Dealer Best Compliance Practices

Regulatory agencies are looking closely at broker-dealer activity. The first line of defense against further scrutiny is the maintenance of appropriate policies and procedures. General best practices include:

- Maintaining complete and up-to-date manuals and policies that are tailored to the firm's business model;
- Specifying who is responsible for overseeing/reporting different areas of compliance and the kinds of matters, or "red flags," that must be escalated, both within the compliance department and to senior management;
- Implementing a process for documenting compliance;[25] and
- Ensuring that compliance officers thoroughly document meetings that implicate specific risk controls, such as chaperoned meetings between research analysts and investment bankers.

As discussed above, in several cases, broker-dealers ran afoul of their supervisory and compliance obligations when they began new business

---

[24] U.S. Securities and Exchange Commission, *Staff Summary Report on Examinations of Information Barriers: Broker-Dealer Practices Under Section 15(g) of the Securities Exchange Act of 1934*, (Sept. 27, 2012), *available at* http://www.sec.gov/about/offices/ocie/informationbarriers.pdf; *see id.*, Appendix B (summary list of effective practices). *FINRA 2013 Examination Priorities Letter*, at 5 (Jan. 2013), *available at* http://www.finra.org/web/groups/industry/@ip/@reg/@guide/documents/industry/p197649.pdf (highlighting the following six risk controls:

> [1] routine review of electronic communications of personnel within business units that may come into possession of material, non-public information during the normal course of business, such as investment banking and research departments; [2] maintaining appropriate information-barrier policies and procedures that are designed to limit or restrict the flow of material, non-public information within the firm to employees on a "need-to-know" basis; [3] monitoring employee trading activity both inside and outside the firm to identify suspicious activity; [4] conducting regular reviews of proprietary and customer trading in securities that are placed on a watch/restricted list; [5] conducting employee training with respect to the use and handling of material, non-public information; and [6] a process for identifying suspicious customer trading in securities of their employer or corporate affiliates").

[25] *See In the Matter of Janney Montgomery Scott LLC*, Admin. Proceeding No. 3-14459, 2011 SEC LEXIS 3166 at 5 (July 11, 2011), *available at* http://www.sec.gov/litigation/admin/2011/34-64855.pdf.

ventures. To avoid liability as a result of such transitions, broker-dealers should consider the following guidance:

- Ensure interim procedures are in place;
- Do not adopt previous/older procedures wholesale—tailoring is important;
- Update procedures as business developments occur; and
- Include procedures to train staff and guide employees on the new system.

Information Barriers

Maintaining appropriate information barriers is essential to protect MNPI. Below are suggestions that can be used to assist in a review of firm policies and procedures, subject to variation depending upon broker-dealer size and business model.

Personnel Controls

- Limit access to MNPI on a need-to-know basis;
- Identify which internal groups have access to MNPI and evaluate whether the controls in place prevent misuse of information;
- Categorize employees vis-à-vis information barriers ("walls"), such as: above the wall,[26] behind the wall, wall straddlers/pre-cleared, wall crossing approvers, public side (ad hoc over the wall);[27]

---

[26] For example, firms should note that glass walls may allow visual access to information.

[27] These categories are somewhat self-explanatory, as they relate to an employee's relationship to information barriers. They are often used in conjunction with the "private-side" and "public-side" distinction, which differentiate between areas of the broker-dealer that have ongoing access to MNPI (private-side) and those that have restricted or monitored access to MNPI (public-side). Private-side actors are generally restricted from personal and firm trading in securities for which the group has MNPI, regardless of whether the individual employee has actual knowledge. Private side groups typically include: Investment Banking, Credit, Capital Markets, Syndicate (and origination functions generally), certain Investment Groups, and support and control personnel supporting these areas. Public-side groups, on the other hand, do not have regular access to MNPI and can trade in securities for which the broker-dealer has MNPI as long as the individual trader has not had access to the information. If a public-side employee/group does receive access, those people are supposed to be identified as "over-the-wall" for that corporation/security and restricted from trading. Most Sales and Trading groups are public-side. Some consider Research to be as well—however Research may have MNPI, and therefore physical barriers between Research and Sales and Trading may be advisable despite both being classified as public-side. U.S. Securities and Exchange Commission, *Staff Summary Report on Examinations of Information Barriers: Broker-Dealer Practices Under Section 15(g) of the*

- Maintain written procedures governing potential interactions between research analysts and traders, ensuring that relevant terms are defined so that employees are not confused; [28]
- Maintain a MNPI disclosure reporting and monitoring requirement for above-the-wall executives and others in such a category;[29] and
- Be mindful that groups outside of those traditionally thought to receive MNPI may still be exposed to it; for example, the credit department of a broker-dealer may need to have in place procedures providing for its reporting of MNPI to the Control Room.[30]

Information Controls

- Put in place processes that differentiate between types of MNPI based on the nature of the information or where it originated;
- Tailor "exception" reports that take into account the different characteristics of MNPI;
- If information is relayed to a parent organization, evaluate whether the parent has controls over use of the information;
- Have clear guidelines on the use of customer trading information in developing market color; and
- Consider implementing trees or information boxes as a way to manage conflicts within a given barrier.

Physical Access Controls

- Monitor access rights for key cards and computer networks to confirm

---

Securities Exchange Act of 1934, at 17-18 (Sept. 27, 2012), *available at* http://www.sec.gov/about/offices/ocie/informationbarriers.pdf.

[28] *See Goldman Sachs*, 2012 SEC LEXIS 1189, at 6 (describing confusion over what constituted "short term" trading issues in context of firm's information dissemination policy, which allowed analysts to share "short term" ideas with selected clients and firm traders instead of broadly disseminating information as was normally required).

[29] Some broker-dealers maintain an "above-the-wall" classification for persons, mainly senior executives, who are deemed neither public- nor private-side, such that MNPI is provided to them on a "need-to-know" basis without going through the over-the-wall process. The SEC has expressed concern about the use of the "above-the-wall" category, and firms should consider stronger controls over these personnel. U.S. Securities and Exchange Commission, *Staff Summary Report on Examinations of Information Barriers: Broker-Dealer Practices Under Section 15(g) of the Securities Exchange Act of 1934*, 6, 18 (Sept. 27, 2012), *available at http://www.sec.gov/about/offices/ocie/informationbarriers.pdf*.

[30] Most broker-dealers centralize the management of the information barriers program into one group within the Compliance Department. The group is interchangeably referred to as the "Control Group" or the "Control Room."

that only authorized personnel have access to sensitive areas;

- Put in place adequate physical barriers, particularly over Investment Banking, Credit, Corporate Capital Markets and Syndicate, Private Equity, Research covering corporate issuers, Conflicts, and the Control Room;[31]
- Minimize potential for information to be seen via computer screens;
- Institute appropriate printing and production procedures that limit interaction between public- and private-side areas and ensure that those picking up printing job are the designated recipients;
- Properly dispose of confidential documents; for example, shredding all paper from private-side may prevent inadvertent disclosures;
- Systematically review employee transfers from private- to public-side business units, with a view to limiting the possible misuse of MNPI; and
- Systematically review employee transfers from private- to public-side business units, with a view to limiting the possible misuse of MNPI.

Electronic Access Controls

- Implement automated systems limiting access to information, such as through shared network drives that only provide access to approved deal members;
- Disable the ability to download information from computers to removable storage;
- Limit access in public areas to the Investment Banking computer system (i.e., no remote log-ins);
- Require that requests to download information be approved by a supervisor and forwarded to the appropriate group;
- Prevent documents from being downloaded/printed when accessing network remotely;
- Minimize misdirected emails, by: having private-side employees affirmatively identify emails as appropriate to be sent outside of the department or outside of the broker-dealer; turning off the autocomplete function of email systems to require employees to type in the full email address; and creating pop-ups to identify to the employee that the email was being sent externally;

---

[31] For example, firms should note that glass walls may allow visual access to information.

- Put in place electronic systems or barriers that prevent exposure to MNPI; for example, ensure that personnel cannot access non-displayed liquidity when conducting error trading;[32]
- Block Internet chat rooms and third party messaging services, where information could be shared improperly; and
- Document activity and have written procedures and an audit trail for any virtual data rooms, if used.

Monitoring and Surveillance of Communications

Communication surveillance systems should be tailored, continuously updated, and functional for the company's needs. For example, FINRA found that a firm's email review system was inadequate to prevent information barrier violations because the keywords used to identify suspicious emails were not sufficiently comprehensive or up-to-date.[33] Advisable policies to ensure proper monitoring include:

- Assess content of email, not solely sender and recipient;
- Review internal emails, especially emails between private- and public-side groups;
- Monitor internal communications made through chat rooms or other messaging services;
- Monitor emails within control functions with access to MNPI, including Compliance and IT; and
- Conduct targeted reviews when an "internal use only" document is sent outside the firm or for large attachments sent to generic internet email domains.

Monitoring and Surveillance of Trading Activity

Monitoring trading activity by the firm, its employees, and its customers is essential to prevent and detect insider trading by broker-dealer personnel and customers, and was a common area of SEC and FINRA scrutiny.[34] Broker-dealers should consider the following procedures:

---

[32] *In the Matter of New York Stock Exchange LLC, NYSE Arca, Inc., NYSE MKT LLC f/k/a NYSE Amex LLC, and Archipelago Securities, L.L.C, Admin*. Proceeding No. 3-15860, 2014 SEC LEXIS 1526 (May 1, 2014), *available at* http://www.sec.gov/litigation/admin/2014/34-72065.pdf.

[33] *In the Matter of Rodman & Renshaw, LLC, William A. Iommi*, AWC 20110260605 (Aug. 22, 2012), *available at* http://disciplinaryactions.finra.org/viewDocument.aspx?DocNb=32224.

[34] *See e.g.*, *In the Matter of J.P. Turner & Company, L.L.C.*, AWC 2011025756301 (Apr. 21, 2014), *available at* http://disciplinaryactions.finra.org/viewDocument.aspx?DocNb=35714.

Review Procedures

- Monitor employee trading activity both at and away from the firm by, among other things, obtaining and reviewing duplicate transaction requests and employee account disclosure forms;
- Ensure the surveillance system compares movement in securities price with trade in employees accounts;
- Implement pattern-based surveillance that assesses historical patterns or accumulations of positions over time, ensuring that trading is evaluated based on potential scenarios that could take advantage of MNPI;
- Expand reviews for potential misuse of confidential information to include trading that goes beyond equities and options, that is, including credit default swaps, equity or total return swaps, loans, components of pooled securities such as unit investment trusts and exchange-traded funds, warrants, and bond options;
- Have a process for identifying when private corporations become public corporations to allow for proper surveillance;
- Confirm that procedures for review are being followed to ensure that employees are disclosing their accounts in accordance with NASD 3050(c);
- Make sure that resources are adequate to ensure that enough employees are reviewing trading; and
- Conduct thorough and robust AML testing—including findings and recommendations.

Practices to Ensure Comprehensive Review

- Develop system that automatically notifies the Control Room when a security may need to be placed on a monitoring list based on information entered into computer systems used for deal management or for conflicts checks;
- Have a process to test whether appropriate information is in fact being placed on lists;
- Review pipeline reports, commitment committee minutes, confidentiality agreements, access reports for electronic information, or news articles that reference the broker-dealer, to identify potential MNPI possession that should be monitored;
- Conduct look-back reviews of trading activity that take into account possible delays in relaying information to the control room—such as reviewing the few weeks prior to placement on the watch list or a

special purpose review when a delay in placement was identified;

Watch and Restricted List Policies

In addition to creating a watch/restricted list, broker-dealers should confirm that such a list is adequately monitored and properly utilized. Firms should ensure that their watch/restricted list procedures:

- Provide clear/complete guidance regarding the timing and basis for adding a company to the watch or restricted lists;
- Identify specific triggers for updating the list;
- Adopt clear guidance for employees on when they should notify compliance about trading that could implicate the watch/restricted list;
- Keep items on the list until the transaction closes, as additional MNPI regarding the transaction may be received even after it is made public;
- Ensure that if employees serve on boards, those companies are placed on a restricted/watch list; and
- Implement guidelines on materiality determinations, such that if a transaction is deemed immaterial, the basis of that determination is documented and any specific factors used to assess materiality are listed.

Broker-dealers may also want to keep in mind that simply disseminating a watch/restricted list may be ineffective for high volume traders. Other methods for ensuring the information is properly heeded include: coding order entry systems; pop-up notices in the trading systems; or hard blocks in trading systems that require a code from the compliance department to complete the transaction.

Training

FINRA has shown it will conduct a thorough investigation into broker-dealer insider-trader training. In one case, FINRA examined the number of minutes the firm's supervisors spent at a compliance meeting discussing specific procedures. It found that, for example, fourteen minutes spent on email review and surveillance procedures and three and half minutes on the interaction of the investment banking and research functions was unsatisfactory.[35] Broker-dealers should think critically about the amount of time spent on training to ensure it adequately addresses relevant risks. After employees have been given proper guidance, broker-dealers should consider having them periodically certify in

---

[35] *See In the Matter of Rodman & Renshaw, LLC, William A. Iommi*, AWC 20110260605 (Aug. 22, 2012), *available at* http://disciplinaryactions.finra.org/viewDocument.aspx?DocNb=32224.

writing their review and understanding of the firm's risk control policies. These certifications should be collected and maintained.

Conclusion

Regulatory agencies are ready and willing to scrutinize any aspect of a broker-dealer's business that can implicate insider trading. To avoid costly regulatory actions, firms must be vigilant in ensuring that their policies and procedures adequately combat the risk of insider trading. The guidance in this article aims to assist compliance officers in reexamining and reevaluating whether the firm's current policies are sufficient in this new regulatory environment.