June 3, 2011

David A. Stawick
Secretary
Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street, NW
Washington, DC 20581

Re: Designation of a Chief Compliance Officer; RIN 3038-AC96; Supplemental Comments

Dear Mr. Stawick:

The Futures Industry Association ("FIA")[1] and the Securities Industry and Financial Markets Association ("SIFMA")[2] (collectively, the "Associations") are pleased to provide additional comments on the proposal by the Commodity Futures Trading Commission (the "CFTC" or the "Commission") to adopt rules (the "Proposed Rules")[3] relating to chief compliance officers ("CCOs") of futures commission merchants ("FCMs"), swap dealers ("SDs"), and major swap participants ("MSPs"). The Proposed Rules would implement certain requirements included in Title VII of the Dodd-Frank Wall Street Reform and Consumer Protection Act (the "DFA")[4] that amend the Commodity Exchange Act (the "CEA"). Our comments today supplement those provided in our joint letter dated January 18, 2011 and confirm several points from the meeting held among representatives of the Associations and staff from the CFTC and the Securities and Exchange Commission ("SEC") on May 17, 2011.

---

[1] The Futures Industry Association is the leading trade organization for the futures, options and OTC cleared derivatives markets. It is the only association representative of all organizations that have an interest in the listed derivatives markets. Its membership includes the world's largest derivatives clearing firms as well as leading derivatives exchanges from more than 20 countries. As the principal members of the derivatives clearinghouses, our member firms play a critical role in the reduction of systemic risk in the financial markets. They provide the majority of the funds that support these clearinghouses and commit a substantial amount of their own capital to guarantee customer transactions.

FIA's core constituency consists of futures commission merchants, and the primary focus of the association is the global use of exchanges, trading systems and clearinghouses for derivatives transactions. FIA's regular members, who act as the majority clearing members of the U.S. exchanges, handle more than 90% of the customer funds held for trading on U.S. futures exchanges.

[2] SIFMA brings together the shared interests of hundreds of securities firms, banks and asset managers. SIFMA's mission is to develop policies and practices which strengthen financial markets and which encourage capital availability, job creation and economic growth while building trust and confidence in the financial industry. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA).

[3] *See* Designation of a Chief Compliance Officer; Required Compliance Policies; and Annual Report, 75 Fed. Reg. 70881 (proposed Nov. 19, 2010) (to be codified at 17 C.F.R. §§ 3.1 & 3.3) (the "Proposing Release").

[4] Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. 111-203, 124 Stat. 1376 (2010).

As discussed in our first comment letter, the Proposed Rules would establish a compliance framework that is significantly different from that currently in place in the financial services industry under the regulations promulgated by other Federal regulators, including the SEC and the several banking regulators,[5] as well as the compliance model adopted by the Commission itself as recently as September 2010.[6]

Our supplemental comments below focus on several main points:

I. The Role of Compliance and the CCO Must Remain Independent from the Role of Business Supervisors

Underpinning many of the comments in our first letter was the broad concern that the Proposed Rules would fundamentally change the role of the CCO by causing the CCO to be deemed a business-line "supervisor." Unless agreeing to manage personnel outside Compliance, the CCO does not have authority over personnel not within his/her direct reporting lines. Therefore, the CCO is not in a position to "enforce"[7] or "ensure" compliance, or, acting alone, "resolve" conflicts of interest. These are the functions of supervisors who are ultimately responsible for making sure that the firm and its employees act in compliance with applicable law. It is the supervisor who has the power to directly control the behavior of business line employees, such as through the traditional powers to hire, fire, reward or discipline personnel. Indeed, the CCO is typically positioned outside the direct line of business for one primary reason: Compliance is an independent and objective control function.

By effectively eliminating the separation between supervision and Compliance traditionally maintained by financial services firms, the Proposed Rules would put an end to the independence necessary to perform the CCO function effectively, and would undermine long-standing regulatory principles.[8] We, therefore, described in considerable detail in our first letter the clear distinctions between the role of the CCO (and Compliance, more generally) and the role of business supervisors, and recommended a number of specific changes to the Proposed Rules.

---

[5] We note that the SEC is also charged with the duty to propose similar rules applicable to security-based SDs and MSPs (*see* Section 764 of the DFA adding Section 15F "Registration and Regulation of Security-Based Swap Dealers and Major Swap Participants" to the Securities Exchange Act of 1934 ("Exchange Act"), as well as Section 765 of the DFA).

[6] The CFTC's retail foreign exchange dealers ("RFED") rule requires each RFED to designate a CCO who must certify that the RFED has in place policies and procedures "reasonably designed to achieve compliance with the Act, rules, regulations and orders thereunder." See 17 C.F.R. § 5.18(j). We note also that the CFTC has published other rules for comment under the DFA that would impose additional obligations on CCOs. We believe that all of these rules should be consistent. *See* our first comment letter, at note 7 and accompanying text.

[7] For this reason, in our first comment letter we objected to the use of the term "enforce" in proposed Section 3.3(a) and proposed alternative language.

[8] Since 1964, the Exchange Act has imposed liability directly on firms and individuals for failure to supervise those employees subject to their supervision who violate securities laws. *See* Sections 15(b)(4)(E) and 15(b)(6) of the Exchange Act. *See also* 17 C.F.R 116.3, the CFTC's Supervision rule.

We note that these critical distinctions are discussed at length in the widely-recognized 2005 *White Paper on the Role of Compliance* ("White Paper"), prepared by the former Securities Industry Association's Compliance & Legal Division, a copy of which is attached hereto as Exhibit A. The purpose of the White Paper was to clarify the critical distinction between (a) a securities firm's general efforts designed to achieve compliance with applicable laws, rules, and regulations, and the specific functions of the Compliance Department in support of those goals, and (b) management's responsibility to supervise, and the Compliance Department's role to monitor and surveil. The White Paper continues to be the model for compliance professionals throughout the securities industry and is relied upon by the industry and regulators, alike. Because many FCMs and some SDs and MSPs are also registered broker-dealers, which have structured their Compliance Departments in keeping with the White Paper and FINRA Rules, we urge the CFTC to harmonize the Proposed Rules with the securities industry approach to the greatest extent possible.

II. "Ensuring" Compliance

"Ensuring" compliance, in the strictest sense of what this phrase could mean, is an unrealistic and unattainable standard. We stated in our first comment letter that the CCO is unable to "ensure" compliance if such term is defined to mean "guarantee" because no one person can guarantee or make sure that the registrant and each and every employee is complying with all provisions of applicable law. The CFTC should make clear that the use of the words "ensure compliance" in Section 731(k)(2)(E) of the DFA does not mean the CCO guarantees absolute compliance by the firm and every employee.[9]

Instead, as we proposed in our first letter, the CFTC should include in its Proposed Rules a provision to interpret this statutory language as follows:

> "*For purposes of the Act and this Section 3.3, the term 'ensuring compliance' shall mean taking reasonable steps to establish, maintain, review, modify, and test the effectiveness of compliance policies as defined in Section 3.1(g).*"

However, if the CFTC is concerned about the role of Compliance in "escalation" of compliance matters to senior levels of management (up to and including the senior officer and/or the Board), then this concept could be expressly stated by amending the proposed definition of "compliance policies" in Section 3.1(g) of the final rule as follows:

---

[9] We also note that proposed Section 3.3(d)(4) discusses the "remediation of non-compliance issues," a clear recognition that no CCO, supervisor, or anyone else will be able to "ensure" complete compliance at all times with all requirements, and that the "reasonableness" standard of the broker-dealer model is more appropriate. Furthermore, proposed Section 3.3(d)(5) discusses "management response" to remediation of noncompliance issues. Not only is this further recognition that some *non*-compliance is inevitable, it also acknowledges that firm *management* has responsibility for implementing supervisory and compliance policies.

> *"(g) Compliance policies and procedures. Compliance policies and procedures means material written policies, procedures, codes (including a code of ethics), safeguards, rules, programs, and internal controls required to be adopted or established by a registrant pursuant to the Act and Commission regulations reasonably designed to achieve compliance with applicable provisions of the Act, Commission regulations or applicable rules adopted by a futures association registered under Section 17 of the Act, <u>including procedures for escalating inadequate management responses to apparent material violations of compliance policies and procedures to the appropriate level of senior management, up to and including the senior officer or the board of directors, of the futures commission merchant, swap dealer, or major swap participant, depending on the facts and circumstances of the issues being addressed.</u>"*[10]

III. <u>"Resolving" Conflicts of Interest</u>

Section 731(k)(2)(C) of the DFA and the Proposed Rules require the CCO to "resolve any conflicts of interest that may arise." In short, the CCO acting alone is not in a position to resolve conflicts. The analysis is similar to what we have suggested above regarding "ensuring" compliance: the responsibility to "resolv[e]" conflicts must be defined in a manner that is both reasonable given the nature of the task and with business and compliance roles assigned in a meaningful way.

"Resolution" of a conflict can take many forms that include at least two high-level alternatives: (1) avoiding the conflict, choosing between one or more undertakings with elements of conflict and foregoing any participation in all but one; or (2) mitigating and managing the conflict, going forward with more than one undertaking but minimizing the effect by establishing robust policies, procedures and supervisory oversight.[11] The choice between these paths, and the choice among possible steps in each path, must take account of many, legitimate commercial elements and judgments. Senior management of the business uniquely can consider those elements and make business judgments on the desired course.

As stated in our first comment letter, we do not believe that, when Congress used the term "resolve," it intended to mean "resolve" in the executive or managerial sense such that the CCO alone would examine the facts and determine and execute on the course of action. We believe Congress intended to mean identify, advise, escalate as appropriate and assist senior management

---

[10] We note that in our first letter, we proposed a number of changes to the definition of compliance policies and procedures. The definition proposed here builds on the definition in our first letter. Underlined text represents the proposed addition to the definition we proposed in our first letter.

[11] *See generally*, Speech by Stephen M. Cutler, Director, Division of Enforcement, Securities and Exchange Commission, before The National Regulatory Services Investment Adviser and Broker-Dealer Compliance/Risk Management Conference, September 9, 2003. Noting, in particular, "[t]he historical success of the financial services industry has been in properly managing these conflicts, either by eliminating them when possible, or disclosing them," Available at: http://sec.gov/news/speech/spch090903smc.htm

in resolving conflicts, and to require putting in place reasonable procedures for the resolution of conflicts. Again, the authority to actually resolve conflicts, like the power to enforce[12] compliance, resides with the firm's senior executives and supervisors. Accordingly, we believe the CFTC should adopt a provision interpreting the term "resolve conflicts" as follows:

> *"For purposes of the Act and this Section 3.3, the term 'resolving any conflicts of interest' shall mean designing a system of conflict identification, assessment and resolution, advising on conflict avoidance or mitigation alternatives, and escalating inadequate management responses to conflicts to senior management, including the senior officer or the board of directors, of the futures commission merchant, swap dealer, or major swap participant."*

Again, as with "ensuring" compliance, Compliance can work with the business to advise on the design of processes as well as individual issues, and must have the ability to escalate any proposed course of action that is not among acceptable courses as well provide additional oversight, backstopping supervisory review of the execution and effectiveness of mitigation efforts. The business is crucial to, among other things, actual conflict identification by creating visibility into business activities, contributing to the assessment of the nature of the conflict, participating in the iterative dialogue around alternative avoidance or mitigation strategies, and exercising the final authority, subject to escalation, to make the business choices that must be made.

The process design, issue-specific and concurrent advice and escalation roles are substantial, multifaceted and meaningful roles for Compliance in conflict resolution. CCOs have a key role, but the job of "resolving" conflicts cannot be exclusively theirs. Section 731(k)(2)(C) does not demand, nor should the CFTC undertake to create, an exclusivity that would weaken the conflict management process at best and render it wholly unworkable at worst.

IV. Annual Report and Certification

In our first comment letter, we requested a number of specific changes to the content requirements for the annual report and noted that the CEO, and not the CCO, should certify the annual report. However, should the CFTC believe that the CCO must make the certification in connection with the annual report, we respectfully submit that, with respect to FCMs, SDs, or MSPs that are registered broker-dealers, the CEO of such FCM, SD or MSP *also* be required to make this certification (similar to that required by the New York Fed in connection with its Primary Dealer Compliance Program).

We offer the following additional comments on the annual report and certification provisions of the Proposed Rules:

---

[12] *See* note 7, *supra*.

A. Harmonization of Rules

As discussed in our meeting with the CFTC and SEC staffs on May 17th, many FCMs and some SDs and MSPs are registered broker-dealers subject to FINRA's CEO certification and compliance report requirements. We, therefore, urge the CFTC to harmonize to the greatest extent possible its Proposed Rules with FINRA Rule 3130 (attached as Exhibit B) to minimize confusion and the burden associated with multiple differing requirements for meeting what is a substantially similar objective, *i.e.*, to see to it that registrants have in place robust and effective compliance programs.

B. Elements of the Annual Report

(i) Subsection (d)(2)

Proposed Section 3.3(d)(2) requires the CCO's annual report to "[r]eview each applicable requirement under the Act and Commission regulations, and with respect to each: (i) Identify the policies and procedures that ensure compliance with the requirement under the Act and Commission regulations; (ii) Provide an assessment as to the effectiveness of these policies and procedures; and (iii) Discuss areas for improvement, and recommend potential or prospective changes or improvements to its compliance program and resources devoted to compliance".

For the reasons discussed in our first comment letter, we respectfully urge that this provision be revised to read as follows (proposed additions underlined; proposed deletions [bracketed]):

> *"Review each applicable requirement under the Act and Commission regulations, and with respect to each: (i) Identify the compliance policies, [and] procedures, and programs that are reasonably designed to achieve [ensure] compliance with the requirement under the Act and Commission regulations; (ii) Provide a[n] risk-based assessment as to the effectiveness of [these] such policies, [and] procedures, and programs; and (iii) Discuss areas for improvement, and recommend potential or prospective changes or improvements to its compliance program and resources devoted to compliance"*

(ii) Subsection (d)(3)

Proposed Section 3.3(d)(3) requires the CCO's annual report to "[p]rovide a statement of certification of compliance with sections 619 and 716 of the Dodd-Frank Wall Street Reform and Consumer Protection Act, and any rules adopted pursuant thereto".

As discussed in our first comment letter, there remain significant open and unanswered questions as to the scope and requirements of Sections 619 and 716 of the DFA – the "Volcker Rule" and the "Derivatives Push-Out" rule, respectively. Additionally, the effective dates of these sections of DFA are significantly later than the Proposed Rules currently being considered by the Commission. Further, under the Volcker Rule, the CFTC is expressly mandated to "consult and

coordinate" with the other members of the Financial Stability Oversight Counsel "for the purposes of assuring, to the extent possible, that such regulations are comparable and provide for consistent application and implementation of the applicable provisions of this section to avoid providing advantages or imposing disadvantages to the companies affected by this section…." As to the Derivatives Push-Out rule, consultation and consideration are also required among the CFTC, SEC and the applicable Federal Banking Agency.

In light of these significant considerations, we wish to re-emphasize that any discussion of the type or nature of certification with respect to these rules, including whether any such certification is feasible or appropriate, should be conducted as part of the Volcker and Derivatives Push-Out rulemaking processes. Consequently, this requirement to certify these provisions should be deleted from the Proposed Rules and the items should be renumbered accordingly.

(iii) Subsection (d)(5)

Proposed Section 3.3(d)(5) requires that the annual compliance report "[d]escribe the financial, managerial, operational, and staffing resources set aside for compliance with respect to the Act and Commission regulations, including any deficiencies in such resources".

Although the CCO can describe the resources of the Compliance Department, the CCO is not in a position to describe the "financial, managerial, operational, and staffing resources" set aside for compliance at the firm more generally. Of course, when known to the CCO and warranted, the CCO should make recommendations to senior management when resources or staffing appear to be inadequate – either within or outside of the Compliance Department. Accordingly, we propose that Section 3.3(d)(5) be revised to read:

> *"Describe any recommendations made to the senior officer or other senior management with regard to financial, managerial, operational or staffing resources set aside for compliance with respect to the Act and Commission regulations."*

C. Certification

Although we appreciate that the CFTC has qualified the CCO's certification to apply to the best of the CCO's knowledge and reasonable belief, we strongly believe that the certification should be subject to a materiality standard, especially since potential criminal liability is attached. Accordingly, we propose that Section 3.3(e)(3) be revised to read as follows (proposed addition underlined):

> "The report shall include a certification by the chief compliance officer that, to the best of his or her knowledge and reasonable belief, and under penalty of law, the information contained in the annual report is materially accurate and complete."

V. Conclusion

We wish to express our thanks to the staff of the Commission and the SEC for meeting with us to understand the industry's concerns and discuss these recommendations. Please consider them in view of the practical experience of the Compliance profession upon which they are based. We are strongly committed to maintaining an independent and effective Compliance function within our industry, and we stand ready to answer additional questions or provide additional assistance in the course of these rulemaking proceedings as appropriate.

Sincerely,

John M. Damgard
President
Futures Industry Association

Kenneth E. Bentsen, Jr.
Executive Vice President
Public Policy and Advocacy
SIFMA

cc: Honorable Gary Gensler, Chairman
Honorable Michael Dunn, Commissioner
Honorable Jill E. Sommers, Commissioner
Honorable Bart Chilton, Commissioner
Honorable Scott O'Malia, Commissioner

Division of Clearing and Intermediary Oversight
Sarah E. Josephson, Associate Director,
Claire Noakes, Attorney Advisor

EXHIBIT A

Securities Industry Association
Compliance & Legal Division
435 New Karner Road Albany, NY 12205
(518) 785-0721 (518) 785-3579, Fax siacl@dgallc.net

November, 2005

Dear *SIA Compliance & Legal Division Member* :

We are pleased to provide you with a copy of a *White Paper on the Role of Compliance* prepared by the Securities Industry Association's Compliance and Legal Division Executive Committee.

As Compliance continues to be a critical part of securities firms' self-regulatory efforts, it is very important that we establish a model for Compliance professionals throughout our industry – *and we believe this White Paper to be just that model.* We believe that this White Paper will provide clarity to the Compliance role, dispel some of the misconceptions within the business and regulatory communities regarding Compliance, and serve as an essential document for all Compliance professionals.

The Division Executive Committee wishes to thank specifically, Gerald Baker and Brent Taylor, who provided the leadership on this most important endeavor. The Division Executive Committee also acknowledges the valuable assistance of Ted Levine and Adam Gogolak of the law firm of Wachtell, Lipton, Rosen and Katz.

We hope that Compliance professionals will find the White Paper a useful guide and tool in their day-to-day activities.

Sincerely,

Paul A. Merolla

Enclosure

The Compliance and Legal Division's members are primarily compliance and legal personnel associated with Securities Industry Association member firms. Among its purposes are enhancement of the integrity and reputation of the securities industry through compliance and legal education and improved communication with industry regulatory bodies.

WHITE PAPER
ON THE
ROLE OF COMPLIANCE

Securities Industry Association
Compliance & Legal Division

WHITE PAPER

ON

THE ROLE OF COMPLIANCE

OCTOBER, 2005

Acknowledgments

Under the overall direction of the Executive Committee of the SIA's Compliance and Legal Division, this White Paper was developed by a working group comprised of members of the Division's Executive Committee, a member of the SIA's Self-Regulation and Supervisory Practices Committee and Gerald Baker, a consultant to the Division, in multiple meetings and discussions that took place during the first five months of this year. In addition to the significant time and effort supplied by our Division and its membership, we wish to acknowledge the valuable assistance provided by *Wachtell, Lipton, Rosen & Katz*, outside counsel for this matter.

WORKING GROUP

Name	Firm
Mr. Gerald Baker	*Consultant*
Mr. Joseph Castro	*Fidelity Investments*
Ms. LaBrena Martin	*RBC Financial Group*
Mr. Allen Meyer	*Credit Suisse First Boston*
Ms. Jill Ostergaard	*Morgan Stanley*
Ms. Pamela Root	*Goldman, Sachs & Co.*
Mr. Scott Shaw	*Bear, Stearns & Co., Inc.*
Mr. Brent Taylor	*JP Morgan Chase*
Mr. Brian Underwood	*A.G. Edwards & Sons, Inc.*
Ms. Amal Aly	*Securities Industry Association*

TABLE OF CONTENTS

THE ROLE OF COMPLIANCE

Securities firms have long made it a priority to adopt and implement robust compliance programs as part of their self-regulatory efforts and good business practices. The Compliance Department plays an important role in securities firms' compliance programs, primarily one of advice, monitoring and training in support of business units and management. The purpose of this paper is to discuss the scope and limits of responsibilities of Compliance Departments in securities firms, and to clarify the distinction between (a) a firm's general efforts designed to achieve compliance with applicable laws, rules and regulations, and the specific functions of the Compliance Department in support of those goals, and (b) management's responsibility to supervise, and the Compliance Department's role to monitor and surveil. This paper will also discuss recent regulatory initiatives impacting compliance programs and, particularly, the role of the Compliance Department.[1]

I. THE COMPLIANCE DEPARTMENT

Background

Stand-alone Compliance Departments developed in the early 1960s. Prior to that time, legal departments generally had responsibility for compliance functions.[2] Compliance Departments developed out of securities firms' need to receive advice and support concerning the broad responsibility to supervise the day-to-day conduct of business unit activities and to have in place policies and procedures reasonably designed to achieve compliance with applicable laws and regulations.

Securities firms and regulators view compliance programs as necessary components of overall sound business practices, not merely an issue of mitigating identified legal and compliance risks.[3] Firms prioritize implementing a "culture of compliance" at every level of their organization as a critical facet of their self-regulatory efforts.[4] In addition to the responsibilities discussed above, effective compliance programs[5] serve the important purposes of identifying potential problems, deterring misconduct and potentially reducing penalties in the event wrongdoing does occur.

A. Organizational Structure of Compliance Departments

While Compliance Departments often carry out similar functions across securities firms, a Compliance Department's role and reporting structure are tailored to the size, resources and business needs of a particular

---

1 The past few years have been dominated by headlines of improper business conduct and conflicts in the financial services industry and corporate America. These scandals have heightened regulatory scrutiny of corporate behavior. Legislative, investigative and regulatory focus on a company's compliance programs has significantly increased, and the introduction of outside monitors and enhanced compliance programs is now a routine remedy in corporate, criminal and civil settlements. The recent mutual fund and investment research settlements, among others, have prompted renewed focus on the compliance function as a means of addressing abuses in the securities industry.

2 O. Ray Vass, *The Compliance Officer in Today's Regulatory Environment*, Practicing Law Institute: Corporate Law and Practice Course Handbook Series, Broker-Dealer Institute (Nov. 12, 1987).

3 *See* Stephen M. Cutler, former Director, Division of Enforcement, U.S. Securities and Exchange Commission, Address at the Second Annual General Counsel Roundtable, Tone at the Top: Getting it Right (Dec. 3, 2004) ("good compliance is good business").

4 *See*, *e.g.*, Lori A. Richards, Director, Office of Compliance Inspections and Examinations, U.S. Securities and Exchange Commission, Address at the Spring Compliance Conference: National Regulatory Services, The Culture of Compliance (April 23, 2003).

5 Effective compliance programs should be proactive in identifying and controlling risks that have the potential to result in violations of law—violations that could result in investor harm and financial and reputational losses to the firm. Compliance should not be viewed as an isolated activity of the firm but rather as an integral part of business activities. Compliance should be the concern of every employee of the firm and should be the mainstay of the firm culture.

firm.[6] A Compliance Department may interact and/or share functions with a variety of different control areas within a firm, including the Legal Department, Internal Audit and Risk Management. The Compliance Department may report to the General Counsel, Risk Management or directly into the Executive office.[7] Further, a Compliance Department may operate in a centralized manner, across functional lines[8] or across business units.

Because the Compliance Department is a control function, Compliance Department personnel generally do not, and should not, report to revenue-generating business units. Even in those cases where a firm dedicates Compliance staff to individual business units, Compliance staff should remain part of the Compliance Department to retain independence from those units. However, the Compliance Department must maintain close ties to senior management, who are accountable for a firm's overall compliance efforts.

No matter what organizational structure is chosen, reporting lines and functions for the Compliance Department should be defined clearly in writing. This includes separating Compliance Department functions from the supervisory functions of line managers, as well as distinguishing the roles of the Compliance Department from other control functions.

Given differences in resources, business activities and management structure, the role and organizational structure of a Compliance Department are likely to differ depending on the size of the firm. In particular, smaller firms may have simpler business structures and therefore may have different needs for dedicated compliance resources,[9] and so their organization and distribution of compliance roles are likely to differ significantly from larger firms.[10] To the extent possible, Compliance Department personnel should not assume any supervisory

---

6 This paper focuses on the role of the Compliance Department within a broker-dealer. In other financial services firms, such as banks, the role of compliance, while similar to that of a broker-dealer, is tailored to banks' business model and the different applicable regulatory requirements. *See* Basel Committee on Banking Supervision, *Compliance and the Compliance Function in Banks* (April 2005). A global financial services firm presents an additional set of challenges including the risks of operating in a global marketplace.

7 Firms must take into account all of the Compliance Department's roles when determining to whom the Compliance Department should report.

8 For example, a Compliance Department may have personnel dedicated to a control room or to anti-money laundering surveillance.

9 The Securities and Exchange Commission ("Commission") has recognized that smaller firms may have limited resources to address compliance issues. *See*, *e.g.*, Final Rule: Compliance Programs of Investment Companies and Investment Advisers, Investment Advisers Act Release No. 2204 (Feb. 5, 2004) (discussing requirements under Investment Advisers Act of 1940 ("Advisers Act") Rule 206(4)-7). "We would expect smaller advisory firms without conflicting business interests to require much simpler policies and procedures than larger firms that, for example, have multiple potential conflicts as a result of their other lines of business or their affiliations with other financial service firms. The preparation of these simpler policies and procedures and their administration should be much less burdensome." *Id.* NASD Rules 3010(c)(3) and 3012 include certain exceptions for firms "limited in size and resources." *See* NASD Notice to Members 04-71 (Oct. 2004). However, it is critical that, as smaller firms grow and develop new products and services, their compliance resources scale appropriately.

10 Some smaller firms with limited resources may find it more efficient to use third-party service providers to provide services and support, including certain routine monitoring and surveillance functions. Outsourcing certain functions can allow small firms to leverage external expertise that they neither have the scale nor the resources to generate in-house. While outsourcing may provide a cost-effective way for some firms to build robust compliance programs, concerns have been raised related to the outsourcing of key compliance functions. *See* Lori A. Richards, Address at the Investment Company Institute/Independent Directors Council, Mutual Fund Compliance Programs Conference, The New Compliance Rule: An Opportunity for Change (June 28, 2004); *see also* Technical Committee of the International Organization of Securities Commissions, *Principles on Outsourcing of Financial Services for Market Intermediaries* (Feb. 2005) (noting both the benefits and challenges of outsourcing by financial services firms). This outsourcing issue should not be confused with the increased use by Compliance Departments of outside vendors' software-based monitoring tools to more effectively monitor and surveil business activities.

responsibility (other than supervising the Compliance Department). If Compliance Department personnel do take on both compliance and management supervisory roles, the responsibilities of each role should be delineated clearly; it should be understood that supervisory responsibility emanates from the management role, not from the compliance role.

Defining and maintaining appropriate roles are especially important in organizations where Compliance Department officials also hold legal counsel positions. Lawyers who also perform compliance functions should make it clear to other employees when they are acting as legal counsel and providing legal advice. This will serve to protect any privileges that might apply to their communications.[11]

B. Typical Compliance Functions

Compliance Department functions have evolved over time as one part of firms' self-regulatory initiatives and to provide support for supervisors in carrying out their management responsibilities. The Compliance Department, among other things, performs an advisory, monitoring and education role to support management's supervisory responsibility and its efforts to achieve compliance with government and self-regulatory organization ("SRO") rules and regulations and firm policies. While there are numerous regulations that provide the foundation for compliance programs,[12] there are few specific guidelines for the particular roles and organization of Compliance Department activities.

The functions of individual Compliance Departments can be numerous and wide ranging and depend on a firm's particular business activities and organizational structure. However, there is a set of general responsibilities or functions normally associated with Compliance Departments. While these functions often reside in the Compliance Department, in some firms they may reside in, or be shared with, other control areas or business units.

1. Advisory

Compliance Department personnel provide regulatory and compliance advice to business and control units on an ongoing basis.[13] These efforts involve responding to questions and issues as they arise and proactively keeping business units apprised of regulatory developments and firm policy changes. In order to facilitate this role, Compliance Department personnel are often placed on trading floors or otherwise physically located in, or adjacent to, business units, both to monitor daily business activities and also to address and advise on issues in real time. Compliance Department personnel, along with other control areas, may be consulted by supervisory personnel and may advise business units on transactions prior to execution.[14] The Compliance Department may be involved in the development of new products and services by providing advice on relevant laws and regulations and developing effective monitoring techniques. Advance consultation and coordination with the Compliance Department will facilitate the completion of these efforts prior to the implementation of the new product or service. The Compliance Department may assist in identifying and addressing conflicts of interest and coordinating adherence to the varying legal requirements or customs in different jurisdictions.

---

11 *See* Michelle Jacko, *The CCO & Legal Counsel Role in One*, Compliance Reporter (Nov. 19, 2004) (suggesting that personnel should title emails "Attorney-Client Privilege Information" and include in the body of emails "As Legal Counsel of this firm, I wish to advise on . . . ." as mechanisms to protect privileges); *see also* Vass, *supra* note 2.

12 *See infra* Part III.

13 In some firms, the Compliance Department may share advisory responsibilities with the Legal Department.

14 Approvals for transactions may depend on a variety of factors apart from whether or not a transaction is consistent with applicable laws and regulations, including business and reputational considerations. Business supervisors should make the final decisions as to transactions, given that they are likely to have more information and to be more familiar with particular situations and, ultimately, are responsible for such matters.

2. Policies and Procedures

A core responsibility of the Compliance Department is to assist management in the development of policies, procedures and guidelines designed to facilitate compliance with applicable laws and regulations.[15] Often, the Compliance Department will help develop the policies and procedures in conjunction with individual business units and other control groups. They will also have primary responsibility for the development of the Compliance Department's own policies and procedures; such procedures are helpful in defining the roles and responsibilities of Compliance Department personnel.

The Compliance Department also helps to update and amend policies and procedures in light of regulatory developments (such as new rules and enforcement and disciplinary actions), as part of self-assessment and internal examinations and/or as a result of business changes. The Compliance Department will also disseminate compliance alerts/notices to business units relating to these developments. Compliance Department personnel should also work with business units so that policies and procedures appropriately reflect new business products, services or trends.

3. Education/Training

The Compliance Department often conducts training and education programs to keep business personnel and other employees apprised of policies and procedures and regulatory events. Training should involve both regularly scheduled updates, as well as additional sessions on an as-needed basis to implement new policies or procedures or to communicate recent regulatory developments and can include e-learning modules as an important supplement to in-person training. Special, enhanced training sessions should be conducted on an as-needed basis for business unit supervisors, as well as for new hires. The Compliance Department should contribute to the development of the Firm Element of the Continuing Education requirement, and assist in administering required continuing education requirements for registered personnel under NASD Rule 1120 and NYSE Rule 345A. The Compliance Department also is generally responsible for preparing materials for, and, in conjunction with business supervisors, conducting, the annual compliance meeting required by NASD rules.[16] In some firms, other control functions, such as Internal Audit or Risk Management, may assist in preparing and delivering materials for the annual compliance meeting.

4. Monitoring and Surveillance

Compliance Department personnel perform a critical ongoing monitoring and surveillance function. This role often involves a detailed review of business activities, as well as surveillance of business transactions and communications, to identify potential issues relating to, among other things, the handling of customer accounts, proprietary trading, employee/employee-related trading and employee communications. Monitoring business activity facilitates ongoing compliance with firm policies and regulatory requirements by helping to identify at their early stages patterns of improper behavior or activities,[17] material or systemic weaknesses and potential product-related problems. Compliance Departments also will test the effectiveness of supervisory procedures, often working with other control functions such as Internal Audit.[18] Compliance Department personnel often develop a risk-based approach to monitoring and surveillance as an effective means to identify problems.

---

15 There are some areas of firms where it may be unlikely that the Compliance Department would be involved in policy drafting, for example, Operations, Systems or Human Resources, except in cases where those policies involve compliance and supervisory policies, or Commission, SRO or State rules and regulations.

16 *See* NASD Rule 3010(a).

17 Many firms offer compliance "hotlines" that allow employees to report compliance problems anonymously.

18 *See* NASD Rule 3010; NYSE Rule 342. The Compliance Department may play a critical role in helping the firm carry out its responsibilities under NASD Rule 3012 and NYSE Rule 342, which require firms to have testing and verification systems, independent of supervisors; firms must designate a Principal to have responsibility for such testing; firms may choose to have the Principal delegate some of these responsibilities to Compliance Department personnel.

Compliance personnel, along with business line management, should escalate "red flags" that arise during monitoring and surveillance. It is critical that Compliance personnel escalate issues to senior Compliance officers or the CCO for providing to business supervisors as appropriate and provide them adequate support to facilitate a prompt resolution of any deficiencies. If Compliance Department personnel perceive a supervisor's response to be insufficient, Compliance Department personnel should follow a defined process for escalating and elevating issues to senior Compliance personnel, business line and senior management and/or the Board of Directors.

5. Business Unit Compliance Reviews

Many Compliance Departments, in conjunction with business units, also proactively review business activities to identify potential regulatory, compliance and reputational risks and to design ways to minimize such risks.[19] These reviews are often shared or coordinated with other control groups in the firm. Regulators now emphasize the Compliance Department's ability to be proactive in assessing and identifying these risks throughout a firm and to assist in the remediation of deficiencies before problems arise.[20] Reviews, other than branch office yearly examinations (see below), should include significant business lines from a risk-based perspective, and relevant operations and technology areas. The review procedures and findings should be documented and reported to management.

An important facet of business unit reviews is branch office examinations.[21] Examinations should be carried out by personnel independent of the office in question. "Surprise" examinations in retail branch offices may be appropriate under certain circumstances, especially where the firm has some indication of inappropriate behavior or inadequate controls.[22] The SROs have also recently placed increased emphasis on independent oversight of producing branch managers as well.[23] Firms must be vigorous about reviewing branch office activity, even if offices have only a few employees or are in remote locations.

6. Centralized Compliance Functions

- ***Control Room Function***

Compliance Department personnel generally operate a firm's "control room" that, among other things, administers information barriers between business units.[24] For example, Compliance personnel maintain watch and restricted lists, and handle wall crossings by firm personnel as necessary and appropriate.

- ***Anti-Money Laundering Program Function***

At many firms, Compliance Departments may also administer anti-money laundering programs.[25] Compliance personnel often are involved in the review of new account openings ("know your customer") and surveil for potentially suspicious customer transactions including patterns of asset and fund movements. They may also administer policies and procedures related to privacy, including the implementation of policies pursuant to Regulation S-P.

---

19 NASD rules require firms to conduct business unit reviews at least annually. NASD Rule 3010(c).

20 *See* Stephen M. Cutler, Remarks Before the National Regulatory Services Investment Adviser and Broker-Dealer Compliance/Risk Management Conference (Sept. 9, 2003).

21 *See* NASD Notice to Members 99-45 (June 1999); *see also* Mary Ann Gadziala, Associate Director, Office of Compliance Inspections and Examinations, U.S. Securities and Exchange Commission, Keynote Address at NASD Branch Office Supervision Conference (July 13, 2004).

22 For example, "the receipt of a significant number of customer complaints, personnel with disciplinary records, or excessive trade corrections, extensions, liquidations, or variable contract replacements" may necessitate a "surprise" examination. NASD Notice to Members 99-45, at 300 (June 1999).

23 *See* NASD Rule 3012; NYSE Rule 342.19.

24 Section 15(f) of the Securities Exchange Act of 1934 ("Exchange Act") requires firms to have written policies and procedures to prevent the misuse of inside information.

25 Anti-money Laundering compliance programs are required by both federal law and SRO rules. *See infra* Part III.

7. Licensing, Registration and Employment-related Functions

Compliance Departments often administer the licensing and registration of the firm and its registered personnel. Compliance personnel may also perform diligence on new or potential employees, checking for disciplinary or complaint history. Their activities also include being involved with advising on disciplinary issues, including terminations, and assisting with proper employee registration/licensing where required. Compliance personnel may advise Human Resources personnel on other employment-related issues.

8. Internal Inquiries and Investigations

The Compliance Department, coordinating as appropriate with the Legal Department and other control areas and outside counsel, plays an important role in the conduct of internal inquiries and investigations into possible violations of Commission, SRO and State securities rules and regulations and firm policies. These inquiries and investigations may arise from information gathered in the Compliance Department (*e.g.*, through monitoring and surveillance), be referred from business units or other areas of the firm, or result from reviewing customer complaints, regulatory inquiries, litigation or otherwise.

When investigations occur, the Compliance Department usually focuses on whether a given activity or transaction violates firm policy and procedures, laws, rules or regulations, or industry standards, and whether appropriate systems are in place to detect and prevent such conduct. The Compliance Department, in conjunction with the Legal Department, often makes a report to senior management on significant findings and provides recommendations on remediation and changes in policies and procedures. Compliance personnel also play an important role in developing any necessary reports to regulators.

9. Regulatory Examinations, Reporting and Investigation

The Compliance Department is an important contact point with regulators, often handling and responding to regulatory inquiries and examinations. This may include reviewing documents and records, arranging meetings with firm personnel and discussing potential findings with examiners. Moreover, firms have a number of review and regulatory reporting requirements handled by the Compliance Department or other control groups. These requirements can include making regulatory filings under Commission or SRO rules and regulations (*e.g.*, Form 13D and 13G filings). Compliance Departments also provide support during regulatory investigations including, among other things, gathering information in response to regulatory requests.

10. Fostering Regulatory Relationships

Compliance Departments should have an ongoing, open relationship with regulators to help shape regulatory policy—providing input on rule proposals, participating in training for regulators and meeting with regulators to share views. Additionally, regulators want Compliance Department personnel to (1) participate in the process of identifying problems, (2) work on appropriate responses when problems are uncovered, and (3) help to establish best practices.[26] For example, in September 2003, Stephen Cutler, then Director of the Enforcement Division of the Commission, challenged financial services firms to review their business activities and relationships for conflicts of interest and to report back to the Commission on the results of their review.[27] In this respect, regulators expect the Compliance Department to assist in identifying areas of potential risk and to make responsive recommendations for appropriate action by the firm and its business principals when issues do arise. Finally, Compliance Department personnel should actively participate in industry trade groups, which provide an opportunity to share best practices and to assist in shaping effective regulatory policy.[28]

---

26 *See* Brooke A. Masters & Ben White, *SEC Wants Fixes, Not Fines*, Wash. Post, Sept. 29, 2004, at E01.

27 Cutler, *supra* note 19.

28 *See* Michael Balale, *NYSE Wants Quarterly Compliance Meetings With Big Firms*, Compliance Reporter (Jan. 14, 2005). At such meetings, the NYSE anticipates discussing business concerns and compliance control issues, which could lead to the development of best practices.

11. Promoting a Culture of Compliance

Senior management and the Board of Directors must set a "Tone from the Top," demonstrating strong support for the importance of the compliance function to the firm and clearly prioritizing compliance goals. An important role of the Compliance Department is to assist senior management and business unit managers in promoting a culture of compliance at the firm. Senior management must put in place the people and systems necessary to achieve compliance. This includes allocating sufficient resources to build effective compliance systems (including technology), creating incentive structures that reward compliant behavior (and penalizing behavior that sacrifices compliance principles), and giving Compliance personnel regular and unfettered access to senior management. If business personnel view compliance as a crucial institutional value, they will value the Compliance Department's role and work with Compliance Department officials to achieve business goals within the constraints of the applicable regulatory framework.[29]

12. Program Assessment: Assessment of Existing Business Activities and Emerging Trends

Effective compliance programs require continuous review and updating, particularly in light of new risks. The Compliance Department must keep apprised of regulatory and business developments to assess how they affect firm policies and procedures, and business activities. As new rules and regulations are proposed, the Compliance Department must evaluate those proposals and their impact on the firm and its compliance program. An important facet of program assessment is the identification and remediation of gaps in supervisory and compliance systems,[30] and the testing and verification of control systems.[31] New regulations have placed responsibility on senior management to certify that processes in place are reasonably designed to ensure compliance with applicable laws and regulations.[32] The Compliance Department necessarily will play an important role in assisting the CEO to certify as to processes and in aiding the design of testing processes required by these new regulations. Also, firms should have in place programs to assess their Compliance Departments. Firms should strive to identify and implement established industry best practices, where appropriate to the firm and its businesses.

13. Chaperoning

As part of the settlement with the Commission and the SROs concerning investment banking and equity research, Legal and Compliance Department personnel of the settling firms are required to chaperone certain communications between research and investment banking personnel, in addition to certain oral communications by research personnel to a firm's sales force in connection with the offering of securities. This role should not create supervisory authority.

C. Coordination with Business Units and Senior Management

1. Interaction and Relationship with Senior Management

Compliance officials need access to senior management to escalate issues properly. While it is the responsibility of management to take appropriate action to ensure that the firm is complying with laws and regulations, the Compliance Department plays an integral support role in helping management to address problems and develop remediation plans. Given the Compliance Department's monitoring and surveillance functions, Compliance personnel are often in a key position to detect potential violations of law or deficiencies in compliance programs. Recent regulatory initiatives have been designed to further empower Compliance Departments and give compliance issues more prominence at the highest levels of organizations,[33] for example,

---

29 *See* Lawrence B. Pedowitz, *et al.*, *A Firm-Wide Culture of Compliance: Seven Best Practices That Can Make a Difference*, Insights, June 2004, at 15.

30 NASD Rule 3010.

31 *See* NASD Rule 3012; NYSE Rule 342.

32 *See* NASD Rule 3013; NYSE SR 2004-64.

33 *See*, *e.g.*, NASD IM-3013 ("[I]t is the intention of both Rule 3013 and this Interpretive Material to foster regular and significant interaction between senior management and the chief compliance officer regarding the member's comprehensive compliance program."); Investment Company Act Rule 38a-1, 17 C.F.R. § 270.38-1 (2005).

by requiring interactions between the Chief Compliance Officer ("CCO") and the CEO, the Board, and other members of senior management. In addition, the CCO should discuss and review with the CEO activities that are the subject of the CEO's annual certification pursuant to NASD Rule 3013. The CCO's relationship with, and support role to, the CEO and other senior management is likely to expand as part of that certification process.

2. Interaction and Relationship with Business Units and Their Supervisors

There should be ongoing communication between the Compliance Department and business units while performing the Compliance Department's advisory and monitoring functions, and in responding to any issues as they arise. Compliance Department personnel should attempt to understand the firm's businesses and how various laws, regulations and policies should be implemented, and identify potential compliance risks within the organization. Often, Compliance personnel are physically located in or adjacent to a business unit, which facilitates information flow between business and Compliance personnel. Business unit personnel should be encouraged to contact Compliance personnel when any questions or potential issues arise.

D. Coordination with Other Control Groups: Risk, Internal Audit and Legal

The Compliance Department carries out control functions in conjunction with other control groups within a firm, such as Internal Audit, Risk Management and the Legal Department. Different firms allocate monitoring, testing and verification responsibilities among the Compliance Department, Internal Audit and Risk Management differently, depending on particular business needs, available expertise and organizational structure. The Compliance Department roles often overlap with, and complement, the activities of these other control groups. These other control groups, however, may have to perform these tasks for different purposes. Accordingly, there is a need for ongoing coordination and sharing of information in order for the control functions to be carried out efficiently and effectively.

1. Interaction and Relationship with Legal/General Counsel's Office

Legal and Compliance Departments personnel usually work closely together.[34] They may share responsibilities in developing policies and procedures, investigating potential misconduct or in providing advice to business personnel. In some firms, the Compliance Department may report to the General Counsel. Critical distinctions exist between Legal and Compliance Departments' roles, however, and firms should understand these distinctions.[35]

Routine reports and examinations provided by the Compliance Department may not be protected by legal privilege.[36] Further, agencies and SROs may require firms to report information concerning potential or discovered rule violations, which are often handled by Compliance Department personnel.[37] In some firms, Compliance officials may also serve in legal positions, and, in that capacity, may provide legal advice to the firm and its personnel. In such instances, attorneys who carry out both Legal and Compliance Department roles should make clear when they are providing legal advice in order to preserve any applicable privileges.[38] Lawyers who

---

34 *See* Vass, *supra* note 2, at *59 (noting the frequent cooperative efforts between Legal and Compliance Departments, including "the investigation of appearances or allegations of improper conduct, resolving major customer complaints involving allegations of sales practice or regulatory violations, and dealing with outside regulatory inquiries or actions."). Vass also notes that under some circumstances personnel presume that compliance staff are also lawyers.

35 *See* Jacko, *supra* note 11 (noting that firms may want to hire outside counsel to aid with compliance testing programs to protect communications concerning actual or potential violations of law).

36 *See* Richards, *supra* note 10.

37 Legal personnel may have similar requirements under Sarbanes-Oxley. *See* Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, § 307, 116 Stat. 745, 784 (2002).

38 *See* Jacko, *supra* note 11. This would be especially important in cases where personnel might perceive a compliance officer to be a lawyer. *See* Vass, *supra* note 2.

provide legal advice, even if located within the Compliance Department, should have their communications and advice protected by the attorney-client privilege. However, Compliance Department personnel performing compliance functions will not have their communications and advice protected by the attorney-client privilege, even if they are lawyers by training.

2. Interaction and Relationship with Internal Audit

Internal Audit generally tests business unit activities and the control environment to determine, among other things, whether they are in compliance with a firm's internal policies and procedures, or with external regulatory or financial accounting and reporting requirements.[39] Internal Audit appraises control systems to assess their efficiency and resource allocations; it also reviews operations to ascertain whether established objectives are being achieved and whether programs are operating as planned.[40] Information uncovered during audits may assist the Compliance Department in assessing programs and developing policies and procedures to address identified deficiencies. As a best practice, Internal Audit should also review the activities of the Compliance Department.[41] Recent regulatory focus on firms' testing and verification procedures for supervisory systems increases the need for Internal Audit and the Compliance Department to coordinate activities closely.[42]

3. Interaction and Relationship with Risk Management

Risk Management, which normally reports to the Chief Risk Officer, identifies and manages risk exposures, including credit, market, transaction processing and operations. Regulators now view compliance risk as an integral part of a company's overall risk management program.[43] The Compliance Department should be alert to risk issues and, if identified, bring them to the attention of Risk Management and work with them in developing remediation steps.

II. FIRM COMPLIANCE PROGRAMS AND THE ROLE OF THE COMPLIANCE DEPARTMENT

A. The Distinction Between a Firm's Responsibility to Comply with Applicable Laws and Regulations and the Role of the Compliance Department

Securities firms have a duty to build effective compliance programs, reasonably designed to ensure compliance with applicable laws and regulations.[44] These compliance programs should be part of a broad firm compliance culture, with sufficient resources to operate effectively and coordinate among all business and control areas within a firm. Compliance programs include a variety of different components, including policies, procedures, training, surveillance, testing, systems and control functions, each with a specific role designed to direct or support the goal of firm compliance. Senior management has the ultimate responsibility for the establishment and maintenance of a firm's overall compliance efforts; business line supervisors have the responsibility to oversee business operations and the authority to control employee activity to achieve compliance with applicable policies and laws.[45]

---

39 In public companies, Internal Audit generally has a direct reporting line to the Audit Committee or an equivalent body.

40 Jeffrey A. Kuchar & Jeffrey I. Ziment, *Sarbanes-Oxley and the Role of the Internal Audit Team*, Chief Legal Executive, Fall 2002, at 19.

41 *See* Securities Industry Association, Internal Audit Division, *Audit Guideline: Compliance Department (Broker-Dealer)* (Jan. 1, 2004).

42 *See* NASD Rule 3012; NYSE Rule 342.

43 Risk management assessments are now being carried out as part of the SEC examinations program. *See* Mary Ann Gadziala, Remarks before the 5th Annual Regulatory Compliance Conference for Financial Institutions, Strengthening Investor Confidence Through Sound Compliance and Risk Controls (Sept. 24, 2003).

44 *See infra* Part III.

45 *See infra* Part II.B.

The role of the Compliance Department is to advise businesses on how to comply with applicable laws and regulations,[46] and to monitor business activity and employee conduct to identify violations (or potential violations) of rules, regulations, policies, procedures and industry standards.[47] Even with the evolving, and in many cases increased, emphasis being imposed on the Compliance Department function,[48] there is a huge difference between the role of the Compliance Department and its personnel, and the overall broad firm responsibility "to comply" with applicable rules and regulations.[49] The Compliance Department plays an integral support function for firm compliance programs, but only senior management and business line supervisors ultimately are responsible for ensuring firm compliance with laws and regulations. Since these different roles are often confused, it is critical to understand and maintain these distinctions.

B. The Distinctions Between the Responsibilities of the Compliance Department and Those of Supervisors and Senior Management Must Be Maintained

The management function in a securities firm, not the Compliance Department function, has the responsibility to supervise business units and to direct firm and employee activities to achieve compliance with applicable laws.[50] Supervisory systems function more efficiently when there are clear lines of authority and accountability to line management within a firm;[51] the nature and limits of the Compliance Department's responsibilities must be clearly communicated to supervisors and senior management. While the Compliance Department, a non-business line function, plays an important advisory and monitoring role within a firm's overall compliance system, it does not have supervisory authority.

Compliance Department personnel are not, in most cases, in a position either to remediate wrongful or potentially wrongful conduct, nor to authorize or approve business transactions; only supervisors have the authority and responsibility to make those judgments. Compliance Department personnel will often provide advice to supervisors in making their judgments. In certain limited circumstances, Compliance Department personnel may have such authority; in those cases the authority has been delegated. There are often limits as to a Compliance professional's ability to detect situations in which employees successfully evade or circumvent compliance systems to engage in improper conduct. Further, Compliance personnel usually do not have the power directly to control the behavior of line employees, such as through the traditional powers to hire, fire, or discipline personnel.

---

46 *See* NASD IM-3013 ("The chief compliance officer is the primary advisor to the member on its overall compliance scheme and the particularized rules, policies and procedures that the member adopts."). Other personnel and control functions play an advisory role as well. *See infra* Part III.

47 Legal, Internal Audit, or other departments within a firm may perform one or more of these monitoring roles.

48 *See infra* Part III.

49 Vass, *supra* note 2 (noting the distinction between the specific roles of Compliance Department personnel and the generic compliance responsibilities of management within firms).

50 *See* NASD IM-3013; *see also*, Letter from the Securities Industry Association, to Barbara Sweeney, NASD, Office of the Corporate Secretary (July 18, 2003) [hereinafter SIA Letter].

> Management has line authority to direct firm activities, enforce firm policies and procedures, and impose sanctions for violations of firm rules when appropriate, up to and including suspension or termination of firm personnel. As such, this function naturally resides with branch managers, line supervisors, and other senior line officers that are registered principals of the firm. Therefore, when we speak of ensuring a culture of compliance within a firm, that authority ultimately rests with the CEO and not the CCO.

51 "[P]rimary responsibility for compliance must be borne by the branch manager as the first line supervisor of sales personnel. Obviously, the same principle applies to line managers other than branch managers; *e.g.*, those supervising trading functions, etc. The important concept is that of direct reporting chains and the inseparable responsibilities and authority of line managers." Vass, *supra* note 2, at *58.

The focus on Compliance Departments is a natural outgrowth of firms' desire to build a culture of compliance. Firms are placing more resources within Compliance Departments. Regulators have urged Compliance personnel to take a more proactive role in firm compliance programs,[52] and have stressed the importance of Compliance personnel having access to senior management.[53] These trends, however, do not represent an attempt to place supervisory authority with Compliance personnel. There is a difference between actions designed to increase support for business line supervisory activities, and the supervisory activities themselves. Even recent rules directly impacting the Compliance Department, such as those requiring firms to designate a CCO, do not create supervisory responsibility.

The proactive role of the Compliance Department should not be viewed as a substitute by business line supervisors for their responsibility to supervise the business of the firm. Business line personnel still retain ultimate authority over, and are ultimately accountable for, business activities when issues arise, and supervisors must remain vigilant in carrying out their responsibilities: "IM-3013 provides that the responsibility for discharging compliance policies and written supervisory procedures rests with the firm's business line supervisors. These supervisors are the persons responsible for executing the supervisory policies and procedures that Rule 3010 requires firms to establish and adopt."[54] However, persons who serve in Compliance Department roles can be subject to enforcement actions by the Commission and SROs in limited circumstances. For example, if a Compliance Department employee violates the securities laws, or aids and abets in such violations, such employee would be dealt with under the statutes and rules in the same manner as any other person subject to the Commission's or SRO's authority.

Most Commission and SRO enforcement actions for failure to supervise have arisen against firms and business line personnel.[55] Only in limited circumstances have the Commission and SROs brought failure to supervise actions against non-line personnel, such as Compliance Department officers.[56] These enforcement

---

52 *See* Lori A. Richards, Remarks to National Society of Compliance Professionals National Membership Meeting, Compliance Professionals Play Proactive Defense (Oct. 18, 2001).

53 *See* NASD Rule 3013.

54 NASD Notice to Members 04-71 n.5. *See* Final Rule: Compliance Programs of Investment Companies and Investment Advisers, Release Nos. IA-2204; IC-26299 n.73 (Feb. 5, 2004)

> Having the title of chief compliance officer does not, in and of itself, carry supervisory responsibilities. Thus, a chief compliance officer appointed in accordance with [Advisers Act] rule 206(4)-7 (or [Investment Company Act of 1940] rule 38a-1) would not necessarily be subject to a sanction by us for failure to supervise other advisory personnel.

See also Vass, *supra* note 2.

55 Prior to 1964 and the enactment of Section 15(b)(4)(E) and Section 15(b)(6) of the Exchange Act [originally numbered as Section 15(b)(5)(E) and Section 15(b)(7)], no law made individuals liable for failure to supervise an employee who committed a securities law violation. However, several laws created liability for broker/dealers for violations by their employees. Task Force on Broker-Dealer Supervision and Compliance of the Committee on Federal Regulation of Securities, *Broker-Dealer Supervision of Registered Representatives and Branch Office Operations*, 44 Bus. Law. 1361 (1989) (discussing history of laws creating liability for both firms and individuals for the wrongful acts of employees). Under the doctrine of respondeat superior, the Commission held firms liable pursuant to Section 15(b)(4)(D) for willful violations of the securities laws by their employees. Firms were held vicariously liable for the underlying employee violations, not for a separate claim of deficient supervision. Even prior to 1964, the Commission found firms liable for deficient supervision, under the theory that by failing to supervise, firms' deficient supervision constituted participation in employees' wrongful conduct. *See In re Reynolds & Co.*, Release No. 34-6273, 39 S.E.C. 902 (May 25, 1960).

56 For a Compliance Department officer to be liable for deficient supervision, the employee who violates a securities law must be "subject to the supervision" of the individual. Exchange Act § 15(b)(4)(E).

actions arise only when Compliance Department personnel have been specifically delegated, or have assumed, supervisory authority for particular business activities or situations, and therefore have "the requisite degree of responsibility, ability or authority to affect the conduct of the employee whose behavior is at issue."[57]

While *Gutfreund* and other deficient supervision cases[58] provide general considerations that the Commission might use in assessing the supervisory authority (or lack thereof) of control persons, including Compliance Department personnel, they give few specifics as to the responsibilities that would expose Compliance officials to supervisory responsibility. However, a broad application of these general considerations would be inconsistent

---

[57] *In re John H. Gutfreund*, Exchange Act Release No. 31554 (Dec. 3, 1992). In *Gutfreund*, the Commission issued a Section 21(a) Report addressing the actions of Salomon Brothers' General Counsel, Donald Feuerstein, after he received notice that a Salomon trader had placed false bids in Treasury auctions. The Commission, citing the unique role that Feuerstein played at Salomon, found that "[o]nce a person in Feuerstein's position becomes involved in formulating management's response to the problem, he or she is obligated to take affirmative steps to ensure that appropriate action is taken to address the misconduct." There have only been a handful of other deficient supervision cases brought against compliance officials, and few after *Gutfreund*. In *In re Michael E. Tennenbaum*, Exchange Act Release No. 18429, 47 S.E.C. 703 (Jan 19, 1982), a General Partner and Senior Registered Option Principal was found to have failed properly to supervise a sales person in a branch office. Although not the salesperson's line supervisor, Tennenbaum had general supervisory authority for options compliance, as well as specific authority to permit sales personnel to open discretionary options accounts. Accordingly, Tennenbaum had the continuing responsibility to ensure that sales personnel did not abuse their control over discretionary accounts. Similarly, in *In re Gary W. Chambers*, Exchange Act Release No. 27963 (April 30, 1990), the Commission found that a Senior Vice President of Compliance and Operations had supervisory authority over certain sales personnel, largely focusing on the firm's administrative structure where Chambers had responsibility to establish and maintain adequate procedures to ensure compliance with relevant laws and regulations, including the responsibility to write a compliance and supervisory procedures manual (which he failed to do adequately). In *In re First Albany Corp.*, Exchange Act Release No. 30515, 50 S.E.C. 890 (March 25, 1992), the Commission found that First Albany's Vice President, General Counsel, and CCO had supervisory authority over a salesperson largely based upon the CCO's general responsibility to ensure that registered representatives complied with firm policy, and the CCO's specific ability to discipline sales personnel for trade violations, including removing commissions or issuing fines.

[58] The NASD has also brought deficient supervision cases against Compliance personnel under Rule 3010. In *In re John A. Chepak*, Exchange Act Release No. 42356 (Jan. 24, 2000), the Commission upheld a failure to supervise action by the NASD against a Director of Compliance, for inadequate supervision of traders who charged inappropriate markups. The Commission noted that the firm's supervisory manual specifically gave supervisory responsibility to the Compliance Department, and to Chepak in particular. In *In re Conrad C. Lysiak*, Exchange Act Release No. 33245 (Nov. 24, 1993), the Commission upheld sanctions by the NASD for failure to supervise. Lysiak, a part-time compliance director for Dillon Securities, failed adequately to oversee trading in a branch office for which he was the listed supervisor. *In re Conrad C. Lysiak*, Exchange Act Release No. 33245 (Nov. 24, 1993) (citing *Gutfreund* and noting that an employee need not have the authority to hire or fire to be a supervisor under NASD rules). In *DBCC* v. *Gallison, et al.*, Complaint No. C02960001 (Feb. 5, 1999), the NASD National Adjudicatory Council upheld a failure to supervise claim against a La Jolla Capital Corporation compliance officer for failing to supervise penny-stock transactions. Though the compliance officer did not have specific supervisory authority over such transactions, the officer was responsible for the firm's supervisory manual and also for the firm's national branch audit program, where he failed to follow up on several red flags concerning penny stock activities. The NASD also recently brought an enforcement action against a Jesup & Lamont compliance officer for failing to detect and prevent improper trading by one of the firm's research analysts, where the compliance officer assumed supervisory responsibility over the analyst. *See* NASD News Release, *NASD Fines Former Jesup & Lamont Research Analyst for Trading Contrary to His Own Recommendations* (Feb. 23, 2005).

with the traditional role of the Compliance function.[59] These enforcement actions suggest that the Commission will find that Compliance Department officials have supervisory authority only in those rare circumstances when officials have authority and responsibility over the conduct at issue.[60] Responsibility may also arise in those limited circumstances where a business line supervisor also performs a compliance function,[61] or in cases where firm policy specifically delegates supervisory authority to the Compliance Department over certain activities (*e.g.*, exclusively approving trades or disciplining certain personnel).[62]

III. EMERGING REGULATORY TRENDS IMPACTING THE COMPLIANCE FUNCTION

While securities firms' compliance functions generally have been built as part of firms' self-regulatory efforts, Commission and SRO regulatory actions have also played a role in influencing the development of the roles and responsibilities of the Compliance Department. In this regard, new regulatory requirements and enforcement settlements have placed increased demands for specific supervisory procedures and systems in securities firms, and have impacted the elements of compliance programs.[63] Regulators are looking to Compliance officials to act "proactively"[64] to detect and prevent wrongdoing, and have urged Compliance personnel to move further beyond their traditional advisory roles.[65]

Specific securities rules and regulations governing supervisory procedures and systems are set against the backdrop of general duties for corporations to comply with applicable laws and regulations. Boards of Directors (or equivalent management bodies) have a general corporate duty to ensure that entities have supervisory and reporting systems adequately designed to detect and prevent illegal activity.[66] Various statutory and regulatory requirements establish the responsibility of a company's Board and senior management to take reasonable steps to ensure that appropriate compliance procedures and systems are in place, and are effectively implemented. For example, under Sarbanes-Oxley, CEOs and CFOs of public companies must certify as to the accuracy of periodic financial reports, as well as to the adequacy of internal controls for financial reporting.[67] Moreover, a mutual fund board must now establish written policies and procedures designed to prevent the fund from violating applicable laws.[68]

---

59 *See* SIA Letter, *supra* note 50; Vass, *supra* note 2, at *58 ("It is inherent in the nature of a business organization that supervisory responsibility can rest only with those who have line management responsibility and authority.").

60 *See In re Arthur J. Huff*, Exchange Act Release No. 29017, 50 S.E.C. 524 (March 28, 1991) (concurring opinion).

61 For example, if the CEO is also the CCO.

62 *See* cases cited *supra* notes 57 and 58. Similarly, supervisory authority may arise from Compliance personnel's participation on a firm committee. Participation on committees allows the Compliance Department to voice its views to management and also keeps compliance apprised of important business activities. Compliance may also provide an important advisory role to committee members in making decisions addressing compliance issues. However, it is important for firms to consider the additional responsibilities that might arise from Compliance personnel participating on committees. The Commission might deem Compliance personnel who are members of *business-related* committees as having supervisory responsibility for committee actions. The Commission may not take the same view of Compliance personnel's participation on *control-related* committees, such as credit or best execution.

63 For an overview of recent measures taken by regulators outside the United States addressing the compliance function, see OICU-IOSCO, Technical Committee of the International Organization of the Securities Commissions, *Consultation Report: Compliance Function at Market Intermediaries* (April 2005) [hereinafter IOSCO Consultation Report].

64 *See* Richards, *supra* note 52.

65 *See* Mary Ann Gadziala, Remarks Before The Bond Market Association's Ninth Annual Legal and Compliance Conference, The Vital Role of Effective Comprehensive Compliance Controls at Broker-Dealers (Feb. 4, 2004).

66 *See In re Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996).

67 Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, § 302, 116 Stat. 745, 777-78 (2002).

68 Investment Company Act of 1940 Rule 38a-1, 17 C.F.R. § 270.38a-1 (2005).

Even when not required by specific rule or regulation, well developed compliance systems can play an integral role in influencing government and SRO actions when problems do arise. The Commission considers an entity's overall compliance efforts in determining whether to bring an enforcement action against an organization for employee misconduct.[69] Similarly, the United States Justice Department's "Thompson Memorandum"[70] cites the presence of a robust and effective compliance program,[71] and any remediation or improved programs implemented in reaction to improper conduct, as important factors considered by the Department of Justice in determining whether to charge an entity.[72] When a corporation does face criminal liability, under the U.S. Sentencing Guidelines, an effective compliance program can mitigate against corporate culpability, thus lessening the sanctions for wrongful behavior.[73]

Numerous laws, regulations and SRO rules have had an influence on the structure of compliance programs within securities firms.[74] There has been a progression over time from provisions that address firms' supervisory

---

69 Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 and Commission Statement on the Relationship of Cooperation to Agency Enforcement Decisions, Exchange Act Release No. 44969 (Oct. 23, 2001).

70 Memorandum from Larry Thompson, Deputy Attorney General, to Heads of Department Components, United States Attorneys, Principles of Federal Prosecution of Business Organizations (Jan. 20, 2003). The memo replaced an earlier memo distributed in 1999.

71 The Department of Justice will focus not only on whether or not a firm has a compliance program in place, but also on whether programs in place are adequately designed to prevent and detect wrongful behavior. *Id.*

72 *See id.* The fact that an individual's wrongful actions violated a firm's compliance policies does not by itself absolve a firm of criminal liability under the doctrine of respondeat superior. *Id.*

73 *See* U.S. SENTENCING GUIDELINES MANUAL ch. 8, § 8B2. (2004) (as amended on Nov. 1, 2004). "To have an effective compliance and ethics program . . . an organization shall (1) exercise due diligence to prevent and detect criminal conduct; and (2) otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law." *Id.* at § 8B2.1.(a)(1)-(2). The guidelines cite seven components of a compliance and ethics program ("program") that, at minimum, are required to meet this standard: (1) organization must establish compliance standards and procedures to prevent and deter criminal conduct, (2) organization's governing body must be knowledgeable about the program and exercise reasonable oversight of the program, high-level personnel must ensure the effectiveness of the program, and specific individuals must be delegated day-to-day operation responsibility for the program, (3) organization must not give authority to an individual that the organization knew or should have known had committed illegal acts or other conduct inconsistent with the program, (4) organization must communicate to its managers and employees the standards and procedures of the program, including through training programs, (5) organization should take reasonable steps to ensure the program is followed (by auditing and monitoring), to evaluate periodically the program, and to have a system whereby agent and employees can report actual or potential criminal conduct, (6) organization should promote the program with appropriate incentives and punishments, and (7) organization should respond appropriately to any detected criminal conduct. *Id.* at 8B2.1.(b). The sections of the U.S. Sentencing Guidelines relating to organizations would seem unaffected by the Supreme Court's recent decision in *United States* v. *Booker*. *See* 543 U.S. , No. 04-104, slip op. at [ ] (Jan. 12, 2005), *available at* http://www.supremecourtus.gov/opinions/04pdf/04-104.pdf.

74 The SRO Consultative Committee of the International Organization of Securities Commissions ("IOSCO") published the results of a survey of the status of the compliance functions for markets and market intermediaries in the jurisdictions of the IOSCO members throughout the world. The results of the survey demonstrate that there is a general requirement for investment service providers to have a compliance officer. The role of the compliance officer varies by jurisdiction and depends upon the business and structure of the particular firm. Despite the differences in job requirements and functions, the responses to the survey demonstrate the worldwide importance of compliance officers to the effective functioning of the securities industry. SRO Consultative Committee of the International Organization of Securities Commissions, *The Function of the Compliance Officer: Study on What the Regulations of the Member's Jurisdictions Provide for the Functions of Compliance Officer* (Oct. 2003). IOSCO's Technical Committee also recently issued a Consultation Report which provides a comparative overview of regulators' expectations for the compliance function across jurisdictions, and requests comment on, among other things, the proper roles, responsibilities, and oversight of the compliance function within financial market intermediaries. *See* IOSCO Consultation Report, *supra* note 63. Appendix A to the Consultation Report includes a list of responsibilities of a compliance program which should be considered by firms. *Id.*

systems reasonably designed to assure compliance with laws and regulations, to more recent provisions addressing the compliance function specifically.[75] Since 1964, the Exchange Act has imposed liability directly on firms and individuals for failure to supervise those employees subject to their supervision who violate securities laws.[76] Firms and individuals can avoid supervisory liability if they have: (a) established procedures reasonably designed to detect and prevent the violation in question and a system to implement such procedures, and (b) implemented such procedures, and there was sufficient reason to believe that they were being complied with.[77]

SROs also have established regulations governing supervisory procedures. NASD Rule 3010 and NYSE Rule 342 require member firms to establish supervisory systems and written procedures reasonably designed to achieve compliance with applicable laws, rules and regulations.[78] Firms should also undertake annual reviews reasonably designed to assist in detecting and preventing violations of, and achieving compliance with, such applicable laws and rules.[79] As noted above, NASD Rule 3013[80] requires CEO certification that the member firm has processes in place to maintain and review compliance policies and procedures.[81] The Commission recently promulgated rules under the Advisers Act and Investment Company Act that require mutual funds and investment advisers to implement policies and procedures reasonably designed to detect and prevent violations of the securities laws.[82]

---

75 *See*, *e.g.*, NASD Rule 3011; NYSE Rule 445.

76 Exchange Act §§ 15(b)(4)(E), 15(b)(6); Advisers Act §§ 203(e)(6), 203(f).

77 Exchange Act § 15(b)(4)(E); Advisers Act § 203(e)(6).

78 *See* NASD Notice to Members 98-38 (May 1998); NASD Notice to Members 98-96 (Dec. 1998); NASD Notice to Members 99-45 (June 1999). In Notice to Members 99-45, the NASD explained that, whereas *compliance procedures* generally cover the applicable rules and policies and describe prohibited practices, "[i]n contrast, written *supervisory procedures* document the supervisory system that has been established to ensure that compliance guidelines are being followed and to prevent and detect prohibited practices." NASD Notice to Members 99-45 (June 1999) (emphasis added). NYSE Rule 342 requires the general partners of member organizations to establish systems of supervisory control and requires member firms to "designate a general partner or principal executive officer to assume overall authority and responsibility for internal supervision and control of the organization and compliance with securities laws and regulations." NYSE Rule 342.19. It also requires development of policies and procedures to ensure adequate review and supervision of producing managers. *See also In re Certain Market Making Activities on NASDAQ*, Exchange Act Release No. 40,900 (Jan. 11, 1999) (firms must appropriately supervise head traders, who themselves have supervisory authority). Firms must also maintain adequate controls over their business activities, including independent verification and testing of those activities. NYSE Rule 342.23.

79 Under NYSE Rule 342, firms also must submit an annual supervision and compliance report to the CEO or managing partner that includes:

> (A) A tabulation of the reports pertaining to customer complaints and internal investigations made to the Exchange during the preceding year. . .,
>
> (B) Identification and analysis of significant compliance problems, plans for future systems or procedures to prevent and detect violations and problems, and an assessment of the preceding year's efforts of this nature, and
>
> (C) Discussion of the preceding year's compliance efforts, new procedures, educational programs, etc. in each of the following areas: (i) anti-fraud and trading practices, (ii) investment banking activities, (iii) sales practices, (iv) books and records, (v) finance and operations, (vi) supervision, and (vii) internal controls.

80 The NYSE has proposed amendments to Rule 342, which contain certification requirements similar to NASD Rule 3013. *See* NYSE SR 2004-64.

81 Also under NASD Rule 3013, and under the proposed amendments to NYSE Rule 342, a member organization must designate and identify a CCO. The CEO must certify that he "has conducted one or more meetings with the [CCO] in the preceding 12 months to discuss such processes." NASD Rule 3013.

82 *See* Advisers Act Rule 206(4)-7, 17 C.F.R. § 275.206(4)-7 (2005); Investment Company Act Rule 38a-1, 17 C.F.R. § 270.38a-1 (2005). Advisers Act Rule 206(4)-7 specifies that "[i]f you are an investment adviser . . . , *it shall be unlawful . . . for you to provide investment advice to clients unless you*: (a) Policies and procedures. Adopt and implement written policies and procedures reasonably designed to prevent violation, by you and your supervised persons, of the Act and the rules that the Commission has adopted under the Act . . ." (emphasis added).

Regulators have also placed increased emphasis on firms' testing and control systems to ensure that supervisory systems and procedures are functioning adequately (independent of supervisory lines of authority).[83]

Apart from general provisions governing supervisory procedures at financial services firms, there are also regulations that address more specific facets of a firm's compliance activities. For example, Section 15(f) of the Exchange Act and Section 204A of the Advisers Act require registered broker/dealers and investment advisers to establish policies and procedures to prevent the misuse of nonpublic information.[84] Further, both the NYSE and NASD adopted anti-money laundering standards in order to set minimal requirements for firms to meet their obligations under USA Patriot Act[85] and Department of Treasury regulations.

Recently adopted rules and regulations may have an even greater impact on the functions and structure of the Compliance Department. Several new rules promulgated by the Commission require advisers and mutual funds to designate CCOs, to outline with particularity their roles and functions,[86] and to establish written policies and procedures reasonably designed to prevent violations of the securities laws.[87] Regulators expect such

---

83 Recently adopted NASD Rule 3012 (effective January 31, 2005) requires member organizations to designate one or more principals who will establish procedures to test and verify that the member's supervisory systems (those adopted in accordance with Rule 3010) are sufficient: "The designated principal or principals must submit to the member's senior management no less than annually, a report detailing each member's system of supervisory controls, the summary of the test results and significant identified exceptions, and any additional or amended supervisory procedures created in response to the test results." The NYSE has introduced similar requirements under NYSE Rule 342.23.

84 The NASD and NYSE have jointly set forth minimum elements of an appropriate information barrier policy for member firms, including the maintenance of watch lists and restricted lists, interdepartmental information barriers and employee training. NYSE/NASD 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).

85 *See* Title III of the USA Patriot Act, 107 Pub. L. 56, 115 Stat. 271 (Oct. 26, 2001); *see also* NASD Rule 3011; NYSE Rule 445. The regulations require member organizations to establish written procedures to ensure compliance with applicable anti-money laundering laws (Bank Secrecy Act) and regulations. Firms must also identify an individual or individuals who will be responsible for implementing and monitoring the firms' anti-money laundering compliance program.

86 *See*, *e.g.,* Advisers Act Rule 206(4)-7, 17 C.F.R. § 275.206(4)-7 (2005); Investment Company Act Rule 38a-1, 17 C.F.R. § 270.38a-1 (2005); NASD Rule 3013. Interpretive materials for Rule 3013 indicate that the CCO should have expertise in the process of:

> (1) gaining an understanding of the products, services or line functions that need to be the subject of written compliance policies and written supervisory procedures; (2) identifying the relevant rules, regulations, laws and standards of conduct pertaining to such products, services or line functions based on experience and/or consultation with those persons who have a technical expertise in such areas of the member's business; (3) developing, or advising other business persons charged with the obligation to develop, policies and procedures that are reasonably designed to achieve compliance with those relevant rules, regulations, laws and standards of conduct; (4) evidencing the supervision by the line managers who are responsible for the execution of compliance policies; and (5) developing programs to test compliance with the member's policies and procedures.

Firms need to have the right resources in place to support the CCO in these functions. In addition, Gene Gohlke, Associate Director of the Division of Compliance Inspection and Examinations, in a speech entitled "A Job Description for CCOs of Advisers to Private Investment Funds" given on May 5, 2005 at the Managed Funds Association Educational Seminar Series 2005, identified a comprehensive list of 24 specific duties or functions that CCOs of advisers should consider performing.

87 "In the past, firms were only required to have written policies and procedures governing a fairly narrow scope of activities–insider trading, privacy issues, proxy voting, codes of ethics and anti-money laundering. Now, the coverage of compliance is comprehensive, as the fund must have written policies and procedures to prevent the fund from violating the federal securities laws. . . . These procedures will be critical tools for your Compliance personnel to be able to perform their jobs effectively." Richards, *supra* note 10.

compliance professionals to look not only for activities that pose regulatory risks, but to identify activities that create potential conflicts of interests or reputational risks.[88]

The Commission has also used enforcement settlements with individual securities firms as a method to achieve enhancement of compliance staffing and procedures.[89] As part of the Commission's recent settlements with investment banks concerning equity research, the firms were required to dedicate Compliance staff to equity research departments and to have legal and Compliance personnel chaperone certain communications between research and investment banking.[90] Further, the Commission's recent settlements with mutual funds and their advisers concerning market timing require:

- establishment of an internal compliance controls committee that will review funds' compliance policies and provide reports to an audit committee.
- establishment of a compliance staff position that will address matters related to conflicts of interest, and
- the chief compliance officer to periodically report breaches of duties and/or securities laws by the firm.[91]

In addition, the Department of Justice's settlement concerning alleged price-fixing by NASDAQ market makers required certain firms to tape record communications by their NASDAQ traders[92] and required Compliance staff continually to review a portion of the tapes.[93]

IV. CONCLUSION

This paper demonstrates the critical importance of a well-staffed, experienced and adequately funded Compliance Department. The Compliance Department continues to be a critical part of securities' firms self-regulatory efforts. A robust and well-managed Compliance Department, coordinating with other control functions, including the Legal Department, Internal Audit and Risk Management, provides an important and wide-ranging role in support of a firm's ongoing efforts to maintain an effective overall compliance program.

New business activities and new regulations have placed increased demands on, and scrutiny of, compliance activities over the past few years. Effective compliance programs help identify potential problems, deter

---

88 *See* Stephen M. Cutler, Remarks before the 2004 Investment Company Institute Securities Law Developments Conference, *Minding Your Ps: Preventing Another Crisis in the Mutual Fund Industry* (Dec. 6, 2004) ("[T]he chief compliance officer has a unique role within the . . . organization in identifying and addressing risks in the organization before they become legal violations, promptly uncovering and remedying compliance failures when they do occur, and fostering a culture of compliance throughout the firm."); *see also* Cutler, *supra* note 19; Gadziala, *supra* note 43.

89 While consensual remedies in firm settlements do not create specific industry requirements, they are still a source of guidance about current Commission views on a subject. *In re Prudential*, Exchange Act Release No. 22,755, 48 S.E.C. 372 (1986) provides an early example of the Commission using its enforcement power to require a change in a firm's Compliance Department. The Commission identified two different situations in which supervisory failures led to securities law violations in Prudential's branch offices. As part of the settlement, the Commission required Prudential to hire an independent outside consultant to make recommendations as to supervisory and compliance procedures, including those related to the Compliance Department's directives to branch managers. Further, as part of the settlement, Prudential agreed to reorganize its Compliance Department, including hiring of a compliance officer and revamping the staff of the Legal and Compliance Departments.

90 *See*, *e.g.*, *SEC* v. *Bear, Stearns & Co.*, Civil Action No. [ ], Addendum A (2003), *available at* http://www.sec.gov/litigation/litreleases/finaljudgadda.pdf.

91 *See*, *e.g.*, *In re Massachusetts Financial Services Co.*, Investment Advisers Act Release No. 2213, Investment Company Act Release No. 26347 (Feb. 5, 2004).

92 *United States* v. *Alex. Brown & Sons, et al. (Nasdaq Market Makers)*, Civil Action No. [ ] ( ).

93 *Id.*

misconduct and potentially reduce penalties in the event wrongdoing occurs. Regulators are looking for Compliance Departments to play an increasingly important role in identifying proactively and responding to potential wrongdoing. Compliance Departments have stepped up their efforts in the face of these increased demands and heightened scrutiny.

Even with recent events and the growing number of functions in the Compliance Department, the responsibility for a firm's overall compliance program remains with senior management. Senior management must be actively and personally engaged in ensuring that a securities firm complies with existing laws, rules and regulations, and in actively promoting a culture of compliance at all levels in a firm.

[THIS PAGE INTENTIONALLY LEFT BLANK]

[THIS PAGE INTENTIONALLY LEFT BLANK]

SECURITIES INDUSTRY ASSOCIATION
COMPLIANCE & LEGAL DIVISION

EXHIBIT B

FINRA

Print

3130. Annual Certification of Compliance and Supervisory Processes

(a) Designation of Chief Compliance Officer(s)

Each member shall designate and specifically identify to FINRA on Schedule A of Form BD one or more principals to serve as a chief compliance officer.

(b) Annual Certification Requirement

Each member shall have its chief executive officer(s) (or equivalent officer(s)) certify annually,[1] as set forth in paragraph (c), that the member has in place processes to establish, maintain, review, test and modify written compliance policies and written supervisory procedures reasonably designed to achieve compliance with applicable FINRA rules, MSRB rules and federal securities laws and regulations, and that the chief executive officer(s) has conducted one or more meetings with the chief compliance officer(s) in the preceding 12 months to discuss such processes.

(c) Certification

The certification shall state the following:

The undersigned is/are the chief executive officer(s) (or equivalent officer(s)) of (name of member corporation/partnership/sole proprietorship) (the "Member"). As required by FINRA Rule 3130(b), the undersigned make(s) the following certification:

1. The Member has in place processes to:

(A) establish, maintain and review policies and procedures reasonably designed to achieve compliance with applicable FINRA rules, MSRB rules and federal securities laws and regulations;

(B) modify such policies and procedures as business, regulatory and legislative changes and events dictate; and

(C) test the effectiveness of such policies and procedures on a periodic basis, the timing and extent of which is reasonably designed to ensure continuing compliance with FINRA rules, MSRB rules and federal securities laws and regulations.

2. The undersigned chief executive officer(s) (or equivalent officer(s)) has/have conducted one or more meetings with the chief compliance officer(s) in the preceding 12 months, the subject of which satisfy the obligations set forth in FINRA Rule 3130.

3. The Member's processes, with respect to paragraph 1 above, are evidenced in a report reviewed by the chief executive officer(s) (or equivalent officer(s)), chief compliance officer(s), and such other officers as the Member may deem necessary to make this certification. The final report has been submitted to the Member's board of directors and audit committee or will be submitted to the Member's board of directors and audit committee (or equivalent bodies) at the earlier of their next scheduled meetings or within 45 days of the date of execution of this certification.

4. The undersigned chief executive officer(s) (or equivalent officer(s)) has/have consulted with the chief compliance officer(s) and other officers as applicable (referenced in paragraph 3 above) and such other employees, outside consultants, lawyers and accountants, to the extent deemed appropriate, in order to attest to the statements made in this certification.

---

[1] Members must ensure that each ensuing annual certification is effected no later than on the anniversary date of the previous year's certification.

• • • Supplementary Material: ----------

.01 Designation of Co-Chief Executive Officers. A member may choose to designate a second co-chief executive officer, provided that each of the two chief executive officers must individually discharge all of the obligations set forth in Rule 3130, and each shall be held responsible for the representations in the certification as if they were the member's only chief

executive officer. Designation of a co-chief executive officer pursuant to this Rule applies only for the purposes of this Rule and has no effect on any other regulatory obligation imposed on a member or its chief executive officer.

.02 Designation of Multiple Chief Compliance Officers. FINRA recognizes that compliance expertise may reside in more than one individual in firms with distinct business segments. Therefore, a member may choose to designate more than one chief compliance officer, provided that (1) each designated chief compliance officer is a principal; (2) the member precisely defines and documents the areas of primary compliance responsibility assigned to each designated chief compliance officer and makes specific provisions for which of the designated chief compliance officers has primary compliance responsibility in areas that can reasonably be expected to overlap; (3) each designated chief compliance officer satisfies all of the requirements of Rule 3130 with respect to his or her defined area of primary compliance responsibility as if that individual was the member's only chief compliance officer and (4) collectively, the designated chief compliance officers have the responsibilities and expertise that enable them to consult with the chief executive officer(s) on the totality of the subject matters required to be addressed in the certification by the chief executive officer(s) under Rule 3130. Thus, for example, a member that chooses to have multiple chief compliance officers is required to conduct one or more meetings annually between the chief executive officer(s) (or equivalent officer(s)) and each designated chief compliance officer, individually or collectively. At each such meeting, the chief executive officer (or equivalent officer) would be required to discuss with each chief compliance officer the required topics, but only as it relates to the particular chief compliance officer's defined and documented area of primary compliance responsibility.

.03 Importance of Compliance Processes. It is critical that each FINRA member understand the importance of employing comprehensive and effective compliance policies and written supervisory procedures. Compliance with applicable FINRA rules, MSRB rules and federal securities laws and regulations is the foundation of ensuring investor protection and market integrity and is essential to the efficacy of self-regulation. Consequently, the certification requirement is intended to require processes by each member to establish, maintain, review, test and modify its compliance policies and written supervisory procedures in light of the nature of its businesses and the laws and rules that are applicable thereto, and to evidence such processes in a report reviewed by the chief executive officer(s) (or equivalent officer(s)) executing the certification.

.04 Content of Meetings Between Chief Executive Officer and Chief Compliance Officer. Included in this processes requirement is an obligation on the part of the member to conduct one or more meetings annually between the chief executive officer(s) (or equivalent officer(s)) and the chief compliance officer(s) to: (1) discuss and review the matters that are the subject of the certification; (2) discuss and review the member's compliance efforts as of the date of such meetings; and (3) identify and address significant compliance problems and plans for emerging business areas.

.05 Role of the Chief Compliance Officer. The periodic and content requirements for meetings between the chief executive officer(s) (or equivalent officer(s)) and the chief compliance officer(s), as well as the pertinent requirements of paragraphs 3 and 4 of the certification, are intended to indicate the unique and integral role of a chief compliance officer both in the discharge of certain compliance processes and reporting requirements that are the subject matter of the certification and in providing a reliable basis upon which the chief executive officer(s) can execute the certification. A chief compliance officer is a primary advisor to the member on its overall compliance scheme and the particularized rules, policies and procedures that the member adopts. This is because a chief compliance officer should have an expertise in the process of (1) gaining an understanding of the products, services or line functions that need to be the subject of written compliance policies and written supervisory procedures; (2) identifying the relevant rules, regulations, laws and standards of conduct pertaining to such products, services or line functions based on experience and/or consultation with those persons who have a technical expertise in such areas of the member's business; (3) developing, or advising other business persons charged with the obligation to develop, policies and procedures that are reasonably designed to achieve compliance with those relevant rules, regulations, laws and standards of conduct; (4) evidencing the supervision by the line managers who are responsible for the execution of compliance policies; and (5) developing programs to test compliance with the member's policies and procedures.

It is the expertise in the process of compliance that makes a chief compliance officer an indispensable party to enable the chief executive officer(s) to reach the conclusions stated in the certification. Consequently, any certification made by a chief executive officer (or equivalent officer) under circumstances where a chief compliance officer has concluded, after consultation, that there is an inadequate basis for making such certification would be, without limitation, conduct inconsistent with the observance of the high standards of commercial honor and the just and equitable principles of trade — a violation of Rule 2010. Beyond the certification requirement, it is the intention of this Rule to foster regular and significant interaction between senior management and the chief compliance officer(s) regarding the member's comprehensive compliance program.

.06 Responsibility for Compliance Functions. The chief compliance officer(s) and other compliance officers that report to the chief compliance officer(s) (as described in the sentence that immediately follows) shall perform the compliance functions contemplated by this Rule, including paragraphs 3 and 4 of the certification. Nothing in this Rule is intended to limit or discourage the participation of other employees both within and without the member's compliance department in any aspect of the member's compliance programs or processes, including those matters discussed in this Rule. However, it is understood that a chief compliance officer and, where applicable, the most senior compliance officers having primary compliance department responsibility for each of the member's business segments, will retain responsibility for the compliance functions contemplated by this Rule, including paragraphs 3 and 4 of the certification.

As may be necessary to render their views and advice, the chief compliance officer(s) and the other officers referenced in

paragraph 3 of the certification who consult with the chief executive officer(s) (or equivalent officer(s)) pursuant to paragraph 4, shall, in turn, consult with other employees, officers, outside consultants, lawyers and accountants.

.07 Effect of Certification on Business Line Responsibility. The FINRA Board of Governors recognizes that supervisors with business line responsibility are accountable for the discharge of a member's compliance policies and written supervisory procedures. The signatory to the certification is certifying only as to having processes in place to establish, maintain, review, test and modify the member's written compliance and supervisory policies and procedures and the execution of this certification and any consultation rendered in connection with such certification does not by itself establish business line responsibility.

.08 Ability of Chief Compliance Officer to Hold Other Positions. The requirement to designate one or more chief compliance officers does not preclude such persons from holding any other position within the member, including the position of chief executive officer, provided that such persons can discharge the duties of a chief compliance officer in light of his or her other additional responsibilities.

.09 Members Without a Board of Directors or Audit Committee. The requirement that a member's processes include providing the report to the board of directors and audit committee (required by paragraph 3 of the certification) does not apply to members that do not utilize these types of governing bodies and committees in the conduct of their business.[2]

.10 Content of Report Documenting Processes. The report required in paragraph 3 of the certification must document the member's processes for establishing, maintaining, reviewing, testing and modifying compliance policies, that are reasonably designed to achieve compliance with applicable FINRA rules, MSRB rules and federal securities laws and regulations, and any principal designated by the member may prepare the report. The report must be produced prior to execution of the certification and be reviewed by the chief executive officer(s) (or equivalent officer(s)), chief compliance officer(s) and any other officers the member deems necessary to make the certification and must be provided to the member's board of directors and audit committee in final form either prior to execution of the certification or at the earlier of their next scheduled meetings or within 45 days of execution of the certification. The report should include the manner and frequency in which the processes are administered, as well as the identification of officers and supervisors who have responsibility for such administration. The report need not contain any conclusions produced as a result of following the processes set forth therein. The report may be combined with any other compliance report or other similar report required by any other self-regulatory organization provided that (1) such report is clearly titled in a manner indicating that it is responsive to the requirements of the certification and this Rule; (2) a member that submits a report for review in response to a FINRA request must submit the report in its entirety; and (3) the member makes such report in a timely manner, i.e., annually.

---

[2] As a part of their process, members must have the report reviewed by their governing bodies and committees that serve similar functions in lieu of a board of directors and audit committee.

Amended by SR-FINRA-2008-057 eff. Dec. 15, 2008.
Amended by SR-FINRA-2008-030 eff. Dec. 15, 2008.
Amended by SR-NASD-2007-049 eff. July 16, 2007.
Amended by SR-NASD-2005-121 eff. Oct. 14, 2005.
Adopted by SR-NASD-2003-176 eff. Dec. 1, 2004.

Selected Notices: 04-79, 07-32, 08-57.