CADWALADER

Cadwalader, Wickersham & Taft LLP
New York London Charlotte Washington Beijing

One World Financial Center, New York, NY 10281
Tel 212 504 6000 Fax 212 504 6666
www.cadwalader.com

Clients&FriendsMemo

Expert Networks and Insider-Trading Probes: Best Practices in Fostering Compliance and Reducing Legal Risks

December 21, 2010

As recent news reports indicate, federal law enforcement agents are investigating insider trading allegations surrounding expert networks and their use by hedge funds and other institutional investors seeking to gain an informational edge when making investment decisions.[1]

The term "expert network" is used to refer to firms that are in the business of connecting clients, principally institutional investors, with persons who are deemed to have special expertise in the client's area of interest. Experts can include academics, scientists, engineers, doctors, lawyers, suppliers, and professional participants in the relevant industry, including in some cases even former employees of the company of interest. These networks can save investors the time, cost, and uncertainty associated with obtaining specialized knowledge on their own. If used properly, expert networks can be a valuable and legitimate research tool that facilitates efficient access by clients to persons with specialized and valued expertise. In the wake of Regulation Fair Disclosure[2] and with the growth of hedge funds, the use of expert networks by institutional investors has seen significant growth in recent years.[3]

The ongoing federal investigations appear focused on whether some expert networks are being used as a conduit for the conveyance of material non-public information to other investors. Given the nature of these investigations, investors that utilize expert networks should be aware that their conduct – however legitimate – could draw the attention of the federal agents conducting these investigations. This scrutiny can have negative consequences for firms. Responding to a government investigation is inherently costly and time-consuming, and if the investigation becomes

---

1 *See, e.g.*, Michael Rothfeld, et. al., *Arrests in Insider Probe*, WALL ST. J., Dec. 17, 2010; Michael Rothfeld, et. al., *Insider-Trading Case Accelerates With 'Expert'-Firm Arrest*, WALL ST. J., Nov. 26, 2010..

2 17 C.F.R. Part 240 ("**Regulation FD**").

3 *See* Gregory Zuckerman & Susan Pulliam, *How an SEC Crackdown Led to the Rise of 'Expert Networks,'* WALL ST. J., Dec. 17, 2010; s*ee also* Integrity Research Associates, GROWTH OF EXPERT NETWORKS IS ACCELERATING (Feb. 2008), summarized at http://www.integrity-research.com/cms/2009/01/28/growth-of-expert-networks-is-accelerating/.

public, the firm could suffer significant reputational damage, regardless of whether the firm is ultimately charged with any wrongdoing.

In light of these developments, firms should be prepared for a possible investigation by ensuring that robust and comprehensive compliance programs relating to the use of expert networks are now put in place. If properly executed, these programs can act as the first line of defense against government scrutiny by demonstrating to authorities that a firm has taken appropriate steps to guard against potential wrongdoing; thereby showing that further investigation is unlikely to reveal violations. Moreover, strong compliance programs can reduce the likelihood of employees engaging in wrongdoing and ensure that, if an investigation nonetheless results, relevant information is organized in a way that allows a firm to respond quickly. Finally, and perhaps most importantly, the presence of a strong and effective compliance program can dissuade the Department of Justice ("**DOJ**") and the Securities and Exchange Commission ("**SEC**") from charging the firm itself with a crime, even if particular employees have violated the law.

To the extent it has not done so already, each firm should be reviewing its policies and procedures relating to both insider trading and communications with expert networks. In undertaking this review, each firm should ensure that its policies and procedures are designed with the following goals in mind:

- avoidance of illegal, as well as questionable, activity;[4]
- prompt identification of problematic activity;
- minimizing the inconvenience of an investigation, should one arise; and
- reducing the likelihood that federal prosecutors and the SEC charge the firm itself with violating the law, even if particular employees have acted improperly.

To assist firms in these efforts, this memo provides (i) an overview of the relevant law regarding the use of material, non-public information, and (ii) a set of suggested compliance practices firms should consider in light of the government's ongoing investigations.

[4] As liability for insider trading ultimately turns on the amorphous standard of whether a "reasonable investor" would consider the information significant in making an investment decision, it is recommended that firms take a broad view of materiality in their treatment of information. This is especially warranted as any deliberation by a prosecutor or jury of a matter will be made with the benefit of hindsight and often against a backdrop of significant profits through the use of such information. Similarly, firms should take a broad view of what might be considered non-public, particularly when receiving information from someone affiliated with an issuer.

II. Legal Overview

A. Background on Insider Trading

In general, insider trading laws prohibit anyone from trading a security on the basis of material, non-public information in breach of a duty of trust or confidence owed directly or indirectly to an issuer, the issuer's shareholders, or the source of the information.[5]

The *sine qua non* of any insider trading claim is material, nonpublic information. Information that is "public" cannot form the basis of an insider trading claim. For example, watching trucks on a public road as they leave a warehouse (as a means to help ascertain the level of demand for a product) cannot form the basis of an insider trading claim. Likewise, information must be material to form the basis of an insider trading claim. "Material" has been defined by courts as information that a reasonable investor would consider significant in deciding whether to trade a company's securities.[6]

The concept of materiality often becomes the central question in an insider trading case involving an institutional investor. An investor that assembles multiple pieces of *non-material* information to reach a material conclusion has not violated insider trading laws, regardless of whether the information obtained was nonpublic. Indeed, institutional investors, such as a hedge funds, often piece together bits of public and non-public, *non-material* information to understand the complete picture of a particular company. This is commonly referred to as the "mosaic theory" of investing, and it serves as the basis of a defense to insider trading charges.[7] Investors should be aware, however, that reliance on the mosaic theory can raise difficult questions regarding the materiality of each individual piece of information and whether such pieces are indeed separate, isolated pieces, or merely disaggregated parts of a whole.

B. Theories of Insider Trading

Insider trading violates Section 10 of the Securities Exchange Act of 1934, as amended ("**Exchange Act**"). Section 10 makes it unlawful to "use or employ, in connection with the purchase or sale of any security . . . any manipulative or deceptive device or contrivance in

---

[5] *See* 17 C.F.R. § 240.10b5-1, 10b5-2.

[6] *See Basic v. Levinson*, 485 U.S. 224, 231-32 (1988).

[7] *See, e.g.*, *State Teachers Retirement Bd. v. Fluor Corp.*, 654 F.2d 843, 854 (2d. Cir. 1981) (citation omitted); *see also* Andrew Ross Sorkin, *Just Tidbits, or Material Facts for Insider Trading?*, N.Y. TIMES, Nov. 29, 2010, *available at* http://dealbook.nytimes.com/2010/11/29/just-tidbits-or-material-facts-for-insider-trading/ (discussing use of mosaic theory in Galleon case).

contravention of" rules promulgated by the SEC.[8] Rule 10b-5 under the Exchange Act makes it unlawful to "engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person, in connection with the purchase or sale of any security."[9] Based upon these provisions, the Supreme Court has recognized three general theories of insider trading liability: (1) the classical theory, (2) the tipper-tippee theory, and (3) the misappropriation theory. Importantly, in order to fit within any of these three categories, a person must have violated a duty of trust or confidence.

1. "Classical" Theory. The "classical" theory of insider trading applies when an insider, in violation of a fiduciary duty to his or her company, trades in the securities of the company on the basis of material, non-public information obtained by reason of the insider's position.[10] The SEC has defined the concept "on the basis of" to mean that the person merely was aware of the information at the time of the trade.[11] The classical theory covers the situations where a company executive, board member, or other insider trades in the company's securities (or those of a potential deal partner) in advance of news such as a tender offer, merger, or earnings announcement.

2. "Tipper-Tippee" Theory. The "tipper-tippee" theory imposes liability when (1) the tipper "has breached his fiduciary duty to the shareholders by disclosing the [material, nonpublic] information to the tippee", (2) the tippee "knows or should know that there has been a breach", and (3) the tipper incurred some personal benefit in return.[12] A personal benefit may arise from "a direct or indirect personal benefit from the disclosure, such as a pecuniary gain or a reputational benefit that will translate into future earnings" or by making a "gift of confidential information to a trading relative or friend."[13]

3. "Misappropriation" Theory. The "misappropriation" theory addresses the situation where a person, who is not an insider, lawfully comes into possession of material, nonpublic information, but nevertheless breaches a duty owed to the source of the information by trading on the basis of such information or by conveying the information to another person to trade.[14]

---

[8] 15 U.S.C. § 78j(b).

[9] 17 C.F.R. § 240.10b-5.

[10] *See Chiarella v. United States*, 445 U.S. 222, 228 (1980).

[11] 17 C.F.R. § 240.10b5-1(b).

[12] *Dirks v. S.E.C.*, 463 U.S. 646, 647 (1983).

[13] *Id.* at 664.

[14] *United States v. O'Hagan*, 521 U.S. 642, 652 (1997).

In sum, the legal framework surrounding insider trading is nuanced and comes from a multiplicity of legal sources. Legal strategies regarding insider trading require careful and detailed analysis of particularized facts.

C. Rule 10b5-2: Definition of Duty of Trust or Confidence

In 2000, the SEC defined by rule the relationships that would establish a duty of trust or confidence for purposes of the misappropriation theory.[15] Under Rule 10b5-2, a duty of trust or confidence arises between a recipient of material, nonpublic information and the source when: (1) the recipient "agrees to maintain the information in confidence"; (2) the source and recipient "have a history, pattern, or practice of sharing confidences," such that the recipient knew or reasonably should have known the source expected the information to be kept in confidence; and (3) where the source is the "spouse, parent, child, or sibling" of the recipient.[16] Although the validity of this rule was called into question by the Fifth Circuit Court of Appeals in *SEC v. Cuban*,[17] it is recommended that an institutional investor continue to view the duty of trust or confidence through the lens of Rule 10b5-2 in order to reduce its legal risk.

D. Potential Criminal Charges Associated with Insider Trading

Section 32 of the Exchange Act makes it a crime to willfully violate any provision of the Exchange Act or rule enacted thereunder, including Rule 10b-5. Thus the DOJ, as well as the SEC, can pursue an insider trading violation. In addition to insider trading, the DOJ has the option to bring additional charges that the SEC cannot. These charges include conspiracy, mail and wire fraud, false statements to investigators, and perjury.

In addition, firms should be aware of Section 807 of the Sarbanes-Oxley Act ("**SOX 807**").[18] On its face, SOX 807 appears broader than Rule 10b-5 in a number of important ways. The language of SOX 807 does not include the requirement that there be a "purchase" or "sale" of a security, only that the violation be "in connection" with a security, which is a vague concept that may be subject to challenge. The language of SOX 807 also speaks in terms of any "attempt to execute" a "scheme or artifice" to fraud.

---

[15] *See* Selective Disclosure and Insider Trading, Exchange Act Release No. 33-7881 (Aug. 15, 200), 65 Fed. Reg. 51,715 (Aug. 24, 2000) (adopting, among other things, Regulation FD and Exchange Act Rule 10b5-2).

[16] 17 C.F.R. § 240.10b5-2

[17] *SEC v. Cuban*, 620 F.3d 551, 555-56 (5th Cir. 2010) (questioning, but not deciding, whether Rule 10b5-2 goes beyond the scope of Exchange Act Section 10(b)).

[18] 18 U.S.C. § 1348.

Moreover, the government may argue from the face of the statute that "materiality" in the context of SOX 807 is judged from the perspective of a source company, rather than a reasonable investor.[19] Clients should be aware of these potential issues when crafting a compliance program.

II. Practices to Consider

It is worth emphasizing that there is nothing *per se* illegal about expert networks or obtaining advice from experts through such networks. To the contrary, if used appropriately, these networks provide a valuable and legitimate service to investors by assisting them in the gathering of information that allows them to better understand the industries and issuers in which they are considering investing. Nevertheless, as is true in other contexts of investing, a legitimate source of information can potentially be abused if appropriate compliance procedures are not present.

Firms employing expert networks should take appropriate precautions to minimize the possibility of any wrongdoing. While these precautions must start with the implementation of policies and procedures that address insider trading generally, it is also critical in the current environment that these policies and procedures now specifically and comprehensively address the use of expert networks.

Firms must have policies and procedures addressing insider trading and the interaction with experts and expert networks. At a minimum, these policies and procedures should address: (i) the implementation of information barriers between the firm's public and private sides; (ii) the selection of expert networks and experts, including the firm's due diligence, screening and approval process before a network or expert is utilized; (iii) the interaction with experts, including identification of personnel designated to interact with experts, the manner which interaction is to occur, and the documentation of that interaction; and (iv) the monitoring, surveillance, and supervision of the interaction between the firm and experts and of trading in issuers that are subjects of such interactions. All employees at the firm should be trained thoroughly on the laws governing insider trading and the firm's policies and procedures. A culture should be created whereby employees are encouraged to report to compliance or legal personnel any unusual or problematic activity as well as any information that even arguably constitutes material, non-public information. Firms should document both the processes that they implement as well as the steps personnel take in compliance with these processes thereby creating a detailed record of the firm's efforts to meet its legal and regulatory obligations.

[19] *See United States v. Mahaffy*, No. 05-CR-613, 2006 U.S. Dist. LEXIS 53577 (E.D.N.Y., Aug. 2, 2006), at *39–42.

A. Insider Trading – Information Barriers

Firms should implement adequate information barriers between the firm's public side and private side. Employees that have, or in the course of their normal business dealings are likely to acquire, material, non-public information (*i.e.*, private side employees) should be screened from communications with employees that are involved in trading (*i.e.*, public side employees). Persons in a position to make trading decisions should be trained in distinguishing "non-public" information from "public" information. Additionally, public side employees must understand the need to promptly inform compliance or legal personnel when they are exposed, for any reason, to material, nonpublic information and to refrain from sharing such information or otherwise using or relying on the information. Moreover, because the line between legitimate, public information and material non-public information may be unclear, it is most important that public side employees understand that where any doubt exists as to whether information may be material, nonpublic information and especially where red flags may be present, the employee must promptly consult with appropriate compliance or legal personnel and should not share or otherwise use or rely on such information unless and until such information is approved following a review by compliance and/or legal personnel.

B. Expert Network Procedures

1. Expert Network Compliance Program. Firms should consider instituting a review and approval process to document that the expert network being used employs reasonable practices and compliance efforts. In particular, firms should look to ensure that any expert network used by the firm itself employs a strong screening process. Firms should ask who at the network approves experts, what processes are employed for checking the backgrounds of experts, and may request documentation on the process. Further, firms should consider seeking to review the contractual arrangements between the expert network and their experts, including as to compensation and the representations and warranties provided therein. This process should include a formal review and approval by the firm's compliance and/or legal personnel.

2. Expert-Specific Procedures. In addition to the expert network's compliance program, firms should consider implementing their own independent screening of experts. For example, firms could undertake background checks on certain experts utilized. Any potential "red flags" that appear in the background check could be reviewed by a member of the firm's compliance or legal team before discussions with the expert are held. Consideration should be given to criteria that might cause firms to prohibit the use of an expert or, at the least, subject such approval to stricter scrutiny or the involvement of more senior reviewers within the firm. One important consideration is whether the firm should

prohibit the use of experts who were employed within a certain time frame at a company where the firm is considering investing. Experts who were recently employed by, or affiliated with, the company at issue may have been exposed to material, nonpublic information. Even if the former employees do not possess material, nonpublic information, government investigators may view them with suspicion.

3. Pre-Approvals. Employees should not hold any discussions with experts unless and until they have received approval from their supervisor and the firm. Such approval should be appropriately documented and should reflect the expected scope of the discussions as well as the general purpose behind use of such expert.

4. Documentation of Meetings. Firms are urged to document all discussions or meetings with experts. These records should include, at a minimum, who participated, the expert's current employment, the expert's primary scope or source of knowledge, and the topics covered. Firms also should consider whether to require a member of the compliance or legal team to be present for any discussions with experts.

Further, firms should consider conditioning approval of dealings with particular experts on the expert providing certain commitments prior to or at the opening of the meetings. Firms also may consider requiring all discussions with an expert begin with a discussion in which the expert assents to the following points:

- that the expert understands that the client does not wish to receive material, nonpublic information;
- that the expert has not breached, and will not breach, any confidential agreement or legal duty that the expert has to any party;
- that no one else has breached a legal duty in providing the information to the expert;
- that the expert is not an employee, affiliate or supplier of the issuer that will be discussed on the call;[20]
- that the expert did not pay an employee, affiliate or supplier of the relevant issuer in order to obtain the information;

[20] Where such status is on going, it is recommended that confirmation be obtained from the issuer as to the issuer's knowledge and approval of the expert's activities and any limitations thereon.

- that the information the expert plans to provide was not obtained directly or indirectly by anyone who would not be able to assent to each of the foregoing representations.

At end of the meeting, confirmation should be obtained that nothing discussed changed the assent obtained at the beginning of the meeting.

Documentation from meetings with expert networks should be reviewed and approved by a supervisor. Firms may also wish to consider routine review of such information by a member of the firm's compliance or legal teams. Moreover, all employees that may engage in discussions with experts and their supervisors should be trained to identify problematic answers to scripts or other issues noted during these meetings and should understand the need to bring the same to the attention of compliance or legal personnel for prompt review. No sharing or other use or reliance should be made with respect to any information, pending completion of the review process and, if applicable, any approval process. This is especially important with respect to any information that is flagged as problematic and warranting further review.

Securities of relevant issuers should be added to the firm's watch list to ensure appropriate monitoring of future trading therein.

5. Follow-Up Communications. Communications with experts should be made only through approved means of communication that are tracked by the firm. Firms should prohibit employees from using informal means of communication when interacting with experts. Communications through text messaging, instant messaging, and social networking web sites lend themselves to informality and can easily be taken out of context. Their ambiguity and permanence makes them easy targets for enforcement authorities looking for evidence of inappropriate behavior. Accordingly, employees should be instructed to communicate by phone or in person with experts using the compliance procedures outlined in this memorandum.

To the extent there are any email communications with experts, those communications should be reviewed by compliance personnel or the employee's supervisor. If a message is ambiguous, firms should consider follow-up written communications as necessary to clarify the intent of the message. At the least, firms should document the meaning of an ambiguous phrase to avoid confusion later, after memories have dimmed.

C. Other Procedures

1. Supervision. Supervisory programs should be ongoing and tailored to the particularities of a firm's business. Supervisors should be regularly meeting with the persons they supervise and should be fully informed of each such person's conduct and of the business being conducted. Firms' supervisory procedures should include appropriate documentation of applicable processes, including (i) monitoring of employees' compliance with procedures; (ii) supervisory approval; and (iii) trade monitoring and review. As noted, the purpose of supervisory documentation is to document compliance with internal firm processes. Such documentation should not, however, extend to conclusions as to findings and other evidence of wrongdoing. Instead, such matters should be discussed with legal and/or compliance personnel, who should take responsibility for documenting any reviews, findings, conclusions and the like with respect thereto.

2. Surveillance. Internal surveillance programs should closely monitor the firm's trading positions and strategies. Surveillance should not be limited to firm proprietary accounts but also should include trading that occurs in customer accounts and employees' personal trading accounts. These surveillance systems should monitor for, among other things: (i) significant gains and avoidance of large losses; (ii) patterns of trades in advance of market moving news; (iii) unusual trading methods, products, and the like, and (iv) trades outside the firm's strategy. The firm should investigate any triggering events and document the resulting investigation, including any reasonable explanations for the conduct. While supervisory personnel and traders should be consulted during the course of any such investigation, the investigation should be led by the firm's compliance or legal personnel or outside counsel. All trading in securities related to any expert discussions should be subject to ongoing surveillance.

3. Encourage Questions. Compliance programs should encourage employees to voice concerns and question conduct where doubt exists as to the propriety of trading on certain information. Even firms with the most well-designed and well-operated compliance programs will find it difficult to completely safeguard themselves from all regulatory problems. Creating an atmosphere in which employees feel comfortable raising legal and compliance questions helps firms ensure that they are taking a broad view as to regulatory concerns. And when employee questions are combined with strong policies and procedures in place to address such questions, firms put themselves in a strong position to stay in front of potential compliance problems.

4. Training. Training should be robust, regular, and well-documented (as to coverage and attendance). Such programs should focus on:

- the substance of the law;
- the substance of the firm's procedures;
- the need to self-report or flag problematic issues for further discussion and review.

To the extent possible, training should avoid abstract analysis and instead reflect and speak to real life activities and behaviors faced by firm personnel. Firms should consider more focused training programs for persons that will actually communicate with experts, and such persons' supervisors. Training should emphasize the need to immediately reach out to compliance and legal personnel when there is any doubt as to whether information can be used.

5. Documentation. When government investigators begin asking questions, firms will want to be able to demonstrate the extent to which they strive to comply with the law. For this reason, documentation should be an integral part of a firm's compliance program. Firms will want to display to investigators not only that they have taken steps to inform employees of appropriate policies and procedures, but also that the firm has actively followed through in implementing and enforcing the policies and procedures, and in investigating red flags and other unusual matters.

III. Conclusion

The law of insider trading is nuanced and highly dependent on the facts and circumstances of a particular case. When combined with the costly nature of law enforcement investigations, there are strong incentives in place for firms to implement robust compliance programs to reduce the risk of a government investigation. The government's ongoing investigation of insider trading related to expert networks should remind firms of the importance of a strong compliance and training program covering insider trading and the use of experts.

* * * *

We hope you find this helpful. Please feel free to contact any of the following Cadwalader attorneys if you have any questions about this memorandum.

Steven D. Lofchie	+1 212 504 6700	steven.lofchie@cwt.com
Bradley J. Bondi	+1 202 862 2314	bradley.bondi@cwt.com
Jonathan M. Hoff	+1 212 504 6474	jonathan.hoff@cwt.com
Glen P. Barrentine	+1 212 504 6833	glen.barrentine@cwt.com