Insider Trading Is Back

September 4, 2007

BY CHRISTOPHER J. STESKAL

Remember Ivan Boesky, Dennis Levine, and Michael Milken? Many Wall Street professionals and corporate executives are too young to remember the insider trading scandals of the 1980s. And that is the problem. Insider trading cases against Wall Street professionals and corporate executives are back in a big way.

Following the high profile insider trading cases in the 1980s, there were no SEC enforcement actions against Wall Street professionals between 1990 and 1995, and there were only cases against ten such individuals between 1995 and 2000. Now, in the first half of 2007, the SEC has sued over 20 professionals for insider trading.

Most of the SEC enforcement actions brought this year against Wall Street professionals and corporate executives involve insider trading in advance of mergers and acquisitions. And to be sure, the up tick in mergers and acquisitions activity in the past year has provided fertile ground for SEC enforcement actions. The following are examples:

- On August 3, 2007, the SEC sued a British trader who allegedly made over $3 million in profits through insider trading in options to purchase shares of Petco Animal Supplies, Inc. The trades occurred in advance of an announcement that the company would be acquired by private equity funds.
- On May 17, 2007, the SEC sued a former Oracle Corporation vice president who allegedly traded on confidential information about a series of Oracle acquisitions. The Oracle vice president allegedly obtained the inside information about the acquisitions from his wife, who also worked at Oracle.
- On May 10, 2007, the SEC sued an employee of Morgan Stanley & Co. and her husband for trading on confidential information about the pending acquisitions of three companies.
- On May 3, 2007, the SEC sued an investment banker with Credit Suisse LLC for tipping a Pakistani banker about the pending leveraged buyout of a company.

But the SEC is focusing on more than just insider trading in the context of mergers and acquisitions. The SEC has publicly identified two areas for special scrutiny – hedge funds and so-called Rule 10b5-1 plans. The SEC staff believes that some hedge funds may achieve their eye popping investment returns in part by trading on inside information, and the SEC is searching for a paradigmatic case to bring. The SEC has set up a hedge fund fraud unit, and the number of hedge fund trades referred to the SEC by private market regulators increased from 20 in 2002 to 88 in 2006. The SEC has also noted that corporate executives may be misusing Rule 10b5-1 trading plans by entering and cancelling the plans on short notice, thereby effectively trading on inside information. Rule 10b5-1 plans allow corporate insiders to make trades pursuant to a preset schedule set forth in the plans. Such trades are not subject to blackout periods. The plans do not provide a safe harbor, but rather an affirmative defense to a claim of insider trading. The SEC is looking for an appropriate test case involving the misuse of a Rule 10b5-1 plan to make trades based on inside information.

The recent rash of apparent insider trading is far more sophisticated than the 1980s-style insider trading. Now, insider trading is more likely to occur through a network of traders that includes foreign corporations, relatives, or acquaintances. To combat such insider trading, regulators have banded together. The SEC, NYSE Regulation, the Financial Industry Regulatory Authority, the Options Regulatory Surveillance Authority, and other regulatory bodies have created “scheme teams” to target insider trading rings. Because trading occurs electronically, the regulators are able to parse the data for trading patterns and can readily identify the people or entities that placed the suspicious trades.

After identifying the traders, the SEC will use its subpoena power to try to identify connections between the traders and potential sources of inside information. The unfortunate by-product of these investigations is that many companies are hit with broad SEC subpoenas that are nothing more than fishing expeditions for potential leaks of inside information. For example, the SEC subpoenas may seek all emails over a specified period by anyone who participated in a public announcement that was preceded by unusual trading activity. Although the company may not be the formal target of the investigation, it must bear the cost of complying with the subpoena, which may include hundreds of hours of attorney time spent collecting and reviewing documents.

Given the current enforcement environment, companies should review their insider trading compliance policies and upgrade those policies where appropriate. The goal of any compliance policy is to deter violations of the law, reduce the risk of expensive regulatory enforcement proceedings, and avoid the harm to the company's reputation caused by the initiation of such proceedings. The following provides a high level summary of the key aspects of an effective insider trading policy:

- **Written Policy.** Every company must have a clear written policy prohibiting insider trading.
- **Blackout Periods.** The company should implement "blackout" periods during which corporate insiders are prohibited from trading in the company's securities. We recommend that employees may trade in the company's securities only during the period beginning at the opening of trading on the third business day following the company's widespread public release of quarterly or year-end earnings, and ending at the close of trading on the last day of the second month of the then-current quarter, as long as they are not in possession of material non-public information or subject to any special trading blackout. We also recommend that a company notify the broker that handles the employee option plan of trading blackout periods so that the broker can notify the company if there is a trade during a closed window.
- **Compliance Officer.** There should be one person at the company who is responsible for implementing the compliance program, monitoring blackout periods, preclearing trades, and answering particular questions about compliance. That person can be the general counsel.
- **Training.** The compliance officer should conduct periodic trainings that are interactive, include real life examples of misconduct, and emphasize the risks of trading on inside information, including both criminal sanctions and the harm to a person's reputation.
- **"Need to Know" Culture.** Management should implement a "need to know" culture with respect to sensitive business information, such as, acquisition plans, earnings releases, and significant business developments. The company should track who must have access to such information, and emphasize through training that the information should not be shared with others in the company. The company should set up its information technology system so that access to sensitive business information is limited to the group who needs to have such access.
- **Preclearence of Trades.** We recommend that the company require Section 16 officers and directors to preclear trades in the company's securities with the compliance officer.
- **Rule 10b5-1 Plans.** The company should encourage the use of Rule 10b5-1 trading plans. However, the company should adopt a conservative approach to implementing and changing Rule 10b5-1 plans. We recommend the following guidelines: (1) the plan must be initiated when the insider does not possess material nonpublic information, *i.e.*, during an open window period; (2) the insider cannot execute a trade under the plan for at least 30 days after initiation; (3) the insider must effectively relinquish control over trade execution under the plan; (4) individual trades cannot be modified once the plan has been initiated; (5) the insider cannot trade in the company's securities outside of the plan; (6) except in extraordinary circumstances, the plan should terminate no sooner than 1 year after initiation; and (7) the plan should be disclosed on Form 8-K, and the trades made pursuant to the plan should be disclosed on Form 4.
- **Investigate Leaks.** If the company notices unusual trading activity before a public announcement of sensitive business information, the company should take reasonable steps to investigate and determine the source of the leak. The company should try to get ahead of the problem and remedy any violations of its insider trading policy. If the leak continues, the SEC may begin an investigation and serve a broad document subpoena on the company.
- **Remedy Problems.** The company should have a zero tolerance policy towards insider trading. If the company identifies the source of a leak, or discovers that an employee has violated the company's insider trading policy, the company should take disciplinary action and remedy the violation.

Christopher J. Steskal, Partner, Chair, White Collar/ Regulatory Group, csteskal@fenwick.com, 415.875.2439

©2007 Fenwick & West LLP. All Rights Reserved.

THIS UPDATE IS INTENDED BY FENWICK & WEST LLP TO SUMMARIZE RECENT DEVELOPMENTS IN THE LAW. IT IS NOT INTENDED, AND SHOULD NOT BE REGARDED, AS LEGAL ADVICE. READERS WHO HAVE PARTICULAR QUESTIONS ABOUT THESE ISSUES SHOULD SEEK ADVICE OF COUNSEL.