INSIGHTS

THE CORPORATE & SECURITIES LAW ADVISOR

ASPEN PUBLISHERS

Volume 25 Number 3, March 2011

SECURITIES ENFORCEMENT

Building a Better Insider Trading Compliance Program

With the increasing number of insider trading investigations and enforcement actions, companies carefully should review and strengthen their insider trading compliance programs. They should consider such issues as: what types of actions, information and persons should an insider trading policy cover; how should window/blackout periods be structured; whether existing prohibitions against disclosure of company information are sufficient; whether and how to permit the use of Rule 10b51 trading plans; and to what extent restrictions on hedging, pledging and speculative transactions should be imposed.

By Ari B. Lanin and Daniela L. Stolman

The past few years have ushered in a wave of insider trading investigations not seen since the scandals of the 1980s. The Securities and Exchange Commission (SEC) and other authorities have made it clear that combating illegal insider trading is a top priority. Companies must make the prevention of insider trading a top priority as well. This requires an effective insider trading compliance program that reflects and addresses recent developments.

Ari B. Lanin is a partner, and Daniela L. Stolman is an associate, at Gibson, Dunn & Crutcher LLP in Los Angeles, CA.

This recent wave of insider trading investigations and enforcement actions is significant not only because of the unprecedented level of activity, but also because of the extent to which the legal boundaries of insider trading law are being stretched. With respect to the increased level of activity, the SEC has expanded its enforcement efforts to address trading in everything from treasuries to credit default swaps, and has aggressively pursued the provision of information to expert networks and the trading on that information by hedge funds and others. At the same time, the SEC's actions appear to reflect a gradual erosion of the fiduciary duty element of the offense.

As a result, companies need to take a critical look at their insider trading compliance programs and make revisions both to limit their exposure to insider trading actions and to protect their directors, officers, and employees. Effective programs will not only reduce the instances of actionable insider trading, but also will provide companies with a meaningful defense if they find themselves the subject of a government investigation. To assist companies in their review, set forth below is a brief overview of the relevant law, a summary of recent enforcement developments, and suggestions companies should consider to strengthen their insider trading compliance programs.

Legal Background

In general, insider trading is the purchase or sale of a security on the basis of material non-public

information in breach of a duty of trust or confidence owed directly or indirectly to the issuer, the issuer's stockholders or the source of the information. The statutory basis for insider trading is found in Section 10(b) of the Securities Exchange Act of 1934 (Exchange Act) and Rule 10b-5 thereunder. Under Section 10(b) and Rule 10b-5, it is unlawful, in connection with the purchase or sale of a security, "to employ any device, scheme, or artifice to defraud, to make any untrue statement of material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading, or to engage in any act, practice or course of business which operates or would operate as a fraud or deceit upon any person…"[1]

The Supreme Court has recognized two forms of primary insider trading liability under Section 10(b) and Rule 10b-5: (1) the traditional/classical theory; and (2) the misappropriation theory. Both of these theories also have been used to impose liability on tippers and tippees of inside information.[2] The traditional/classical theory prohibits corporate insiders (whether permanent (*e.g.,* directors, officers, and employees) or temporary (*e.g.,* accountants, lawyers, and consultants)) from trading on the basis of material non-public information.[3] The misappropriation theory prohibits outsiders from trading in violation of a duty owed to the source of the information.[4] This duty may arise from business relationships (*e.g.,* underwriters, accountants, lawyers or consultants)[5] or, as articulated in the SEC's rules, non-business relationships (*e.g.,* information received from a spouse, parent, child, sibling, or other relationship in which there is a history, pattern, or practice of sharing confidential information that results in a reasonable expectation of confidentiality).[6] Thus, both theories share the common requirement of a breach of a fiduciary or fiduciary-like duty. As discussed below, however, recent decisions appear to reflect a gradual erosion of this element of the offense.

A company may be held civilly liable for the insider trading violation of any of its directors, officers, employees, or consultants under either a theory of control person liability or as an aider and abetter of the violation. Control person liability stems from Sections 20(a) and 21(A) of the Exchange Act. Pursuant to Section 20(a), any person who "directly or indirectly, controls any person liable" for an Exchange Act violation will be jointly and severally liable to anyone to whom the controlled person is liable "unless the controlling person acted in *good faith* and did not directly or indirectly induce" the violation.[7] Section 21A(a)(3) of the Exchange Act provides that such a control person may be civilly liable to the SEC for an insider trading violation by a controlled person for the greater of (i) $1.425 million,[8] or (ii) three times the amount of the profit gained or loss avoided as a result of the controlled person's insider trading violation,[9] provided the SEC establishes that the control person *knew or recklessly disregarded* the fact that such controlled person was likely to engage in the acts constituting the violation and failed to take appropriate steps to prevent such act(s) before they occurred.[10] While neither statute defines "controlling person," the legislative history of Section 21A makes clear that a "controlling person" may include employers and any person "with the power to influence or control the direction or the management, policies, or activities of another person."[11]

Aiding and abetting liability is rooted in Section 20(e) of the Exchange Act, which authorizes the SEC to bring actions against a person or entity for aiding and abetting unlawful insider trading. Section 20(e) provides that "any person that knowingly provides substantial assistance to another person in violation of a provision…, or of any rule or regulation issued under this title, shall be deemed to be in violation of such provision to the same extent as the person to whom such assistance is provided."[12] Thus, if a company learns of unlawful insider trading by one of its directors, officers, employees, or consultants and fails to take action to stop it, the company could itself be accused of aiding and abetting in the violation.

In light of the foregoing, the adoption of a robust insider trading compliance program could provide persuasive evidence of a company's good faith and non-inducement of a violation (in response to a Section 20(a) claim) or a company's lack of complicity in a violation (in response to an aiding and abetting claim), and at the same time make it more difficult for the SEC to establish recklessness (under a Section 21A claim).

The Current Enforcement Environment

As noted above, the SEC and other federal authorities have made enforcement of the insider trading laws a priority in recent years, with related investigations reaching unprecedented levels during the latter half of 2010. The breadth of this activity coupled with the tactics being employed highlight the need for a strong and effective insider trading compliance program.

The Duty Element

Among the most significant developments in the current enforcement environment with respect to insider trading are the positions being taken by the regulators with respect to the duty element of the offense. In order to successfully assert a claim for unlawful insider trading, United States Supreme Court precedent first requires the existence of a fiduciary or fiduciary-like relationship (or, in the case of a claim under the misappropriation theory, a "duty of trust or confidence"). The SEC's insider trading claims against each of Oleksandr Dorozhko and Mark Cuban, however, and the court's decisions in those cases, appear to reflect an erosion of that requirement.

In *SEC v. Dorozhko*, the SEC (with the concurrence of the U.S. Court of Appeals for the Second Circuit) removed the duty requirement from certain types of insider trading claims altogether—those in which the allegation is based on an "affirmative misrepresentation." In pursuing its claim against Oleksandr Dorozhko, a Ukrainian national and resident, who traded on confidential quarterly earnings reports on IMS Health that he obtained by hacking into Thomson Financial's servers,[13] the SEC notably did not even argue that Dorozhko's conduct involved a breach of a fiduciary duty in its district court complaint.[14] Further, it vigorously asserted in its appellate brief that "no breach of a duty is required when the defendant engages in affirmatively deceptive conduct, such as lying, acting deceptively, or telling half truths."[15] In a decision that has engendered significant debate, the U.S. Court of Appeals for the Second Circuit accepted the SEC's argument, noting that "none of the Supreme Court opinions considered by the District Court *require* a fiduciary relationship as an element of an actionable securities claim under Section 10(b)."[16]

In *SEC v. Cuban*, the SEC once again chipped away at the duty requirement by turning to its own Rule 10b5-2(b)(1) and arguing that a confidentiality agreement alone creates a duty to disclose or abstain from trading.[17] Here, Mark Cuban, then the largest stockholder of Mamma.com sold off his entire stake after allegedly agreeing to keep confidential certain information regarding the company's planned PIPE offering. While the U.S. Court of Appeals for the Fifth Circuit left unanswered the specific question as to whether a confidentiality agreement in and of itself suffices to establish the duty element of an insider trading offense, it carefully reviewed the facts and circumstances, holding that the allegations as a whole provided more than a plausible basis to find an understanding on Cuban's part that he would not trade.[18] The court's decision to leave this question unanswered, combined with the SEC's expansive position in the case, leaves open the possibility that the SEC may pursue similar actions in the future, and that the courts may ultimately endorse that position.

The Use of Wiretaps

There also has been a change in the underlying tactics and approaches employed by the

regulators to unearth insider trading violations. In the past year and half, prosecutors have for the first time sought to use wiretap evidence to investigate and charge insider trading violations. With the use of such evidence recently being approved by the courts, the path appears clear for regulators to make widespread use of wiretaps in investigating and prosecuting insider trading violations. In the words of one prosecutor, "Recordings are the absolute best evidence, and so we will not shrink from using them."[19] Companies should take heed of these changes. Historically, wiretaps have been reserved for some of the most serious crimes—terrorism, organized crime, and drug trafficking cases—out of concern that aggressive surveillance techniques for lesser crimes would impinge upon the privacy rights guaranteed under the Constitution.[20] By using wiretaps in its insider trading cases, the government has signaled the seriousness with which it views insider trading and the lengths to which it is willing to go to prosecute this crime.

Expert Networks

In 2010, the government began turning its attention to the rise of so-called "expert networks."[21] These networks connect institutional investment managers with expert consultants, including academics, scientists, engineers, doctors, lawyers, suppliers, and professional participants in relevant industries. These networks are of particular concern for public companies as they often include current employees of the companies. For example, the SEC recently charged four technology company employees, who were moonlighting as "consultants" to an expert network firm without the knowledge of their employers, with insider trading for illegally tipping hedge funds and other investors with inside information about their companies. This information included "top line" quarterly revenue and profit margin information, internal sales forecasts, and pricing and volume purchases from suppliers.[22] Bob Nguyen, an expert network employee who recently pled guilty to insider trading, even admitted to the court that one of the goals of the expert network was to recruit current employees of public companies as experts who would provide material, non-public information about their companies.[23]

The proliferation of expert networks, taken together with the heightened interest the regulators have taken in them, highlights the need for companies to expressly prohibit their employees from participating in these networks (whether for compensation or not) and to implement, review and bolster their policies designed to limit external business-related communications.

Updating and Strengthening Your Insider Trading Compliance Program

The events described above highlight the need for all companies to carefully review their insider trading compliance programs. While no program or policy can prevent every violation, an effective program will not only reduce their likelihood and protect a company's directors, officers, and employees from inadvertent violations, but also will provide a company with a strong defense if it finds itself the target of an insider trading investigation. As part of such a review, we suggest consideration of the following principles:

1. ***Use of a Written Policy.*** To the extent your company has not already adopted a standalone written insider trading policy that applies to all directors, officers, employees, and consultants, now is the time to do so. An effective policy should, at a minimum, include the following:
   - A clear, no-nonsense description of the seriousness of the insider trading rules. Recipients should understand that a violation may result in their facing termination, heavy fines, jail time, and other civil and criminal penalties.
   - A plain-English summary of the law, including real-world company-specific

examples of "material information" and a clear explanation of what it means for that information to be "non-public." The policy should indicate that the General Counsel (or other administrator of the policy) is available to answer any questions.

- A statement indicating that it applies to all securities (*e.g.,* common stock, bonds, stock options and other derivative securities), and not just common stock.
- An absolute prohibition on trading or tipping while in possession of material nonpublic information. It should be made clear that this prohibition applies to trading in the securities of *any* company (not just the issuer of the policy), regardless of the existence of a preexisting relationship with or fiduciary duty to that company.
- Extremely limited exceptions to the terms of the policy, potentially including only transactions with the company itself, such as stock option exercises, net exercises (but not broker assisted cashless exercises), vesting of equity awards, and the retention of shares to satisfy tax withholding obligations, as well as certain transactions in the company's 401(k) plan and employee stock purchase plan. Hardship exemptions should not be permitted.
- An obligation to maintain the confidentiality of all company information and an absolute prohibition against disclosing such information to others, including family members, other relatives, business or social acquaintances, and expert networks, unless that disclosure is expressly authorized by the General Counsel and the recipient of that information has agreed to neither use that information nor disclose it to others. Companies also should consider obtaining contractual agreements from third-party business partners, such as suppliers and customers, and financial consultants and advisers prohibiting their disclosure of company inside information.[24] In determining whether to obtain such an agreement from a third-party business partner, consultant, or adviser consider the materiality of the relationship with the relevant third party and the extent to which that party has access to inside information. Companies should also see to it that their Regulation FD policy prohibits unapproved communications with the media, securities analysts, and investors, and coordinate the prohibitions and preclearance procedures in the Regulation FD policy and the insider trading policy.
- The implementation of appropriately tailored window/blackout periods and preclearance procedures for those that are regularly exposed to inside information (discussed in more detail below).
- A statement indicating that the policy applies to directors, officers, employees, and consultants, as well as their family members sharing the same household and the entities they control, such as any corporations for which they are a controlling stockholder or any partnerships for which they are a general partner. While the application of insider trading policies to consultants may present enforceability issues, companies are advised to do what they can to reduce any and all potential violations, including by potentially broadening the reach of their policies to cover consultants.
- A requirement that all directors, officers, employees, and to the extent appropriate, consultants certify to their understanding of the terms of the policy, with annual re-certifications required either as a standalone requirement of the policy or as part of a broader annual code of conduct certification.

2. ***Annual Review/Dissemination.*** Companies should review their insider trading compliance programs annually. This annual review should consider any significant changes in

law, the appropriateness of the trading restrictions in the policy (including the term of the window/blackout policy), and whether the list of individuals subject to trading restrictions or preclearance requirements continues to be appropriate. Significant changes should be summarized, highlighted, and distributed to directors, officers, employees, and consultants.

3. ***Continuing Education.*** Consider implementing annual education programs, especially for directors, officers, and those employees and their assistants regularly exposed to inside information. Such programs should include a review of the company's insider trading policy (highlighting any changes to the policy as described above), relevant law (including a discussion of any recent legal developments), current events and a discussion of questions that frequently arise.
4. ***Administration of the Policy.*** Designate one or more person(s) who are knowledgeable with respect to the securities laws to administer and answer any questions regarding the policy. The contact information for this person should be clearly set forth in the policy itself. To the extent appropriate, this person should address preclearance requests as well.
5. ***Preclearance Policy.*** Companies that have not already done so should strongly consider requiring all directors and officers, certain other employees that are exposed to inside information, and even their assistants (as well as their family members sharing the same household and controlled entities) to preclear trades in company securities. Companies that already have preclearance policies in place should consider whether they apply to the right group of people. In addition, consider implementing additional preclearance related safeguards, such as:
    - A requirement that the requesting director, officer, or employee submit a written preclearance request describing the proposed transaction and certifying that he/she is not aware of inside information;
    - A "use it or lose it" feature, permitting precleared trades to be executed only within a specified number of days after approval (*e.g.,* five days); and
    - A prohibition on the requesting director, officer or employee informing anyone else of the approval or denial of the request.
6. ***Window/Blackout Period.*** Companies that have not already done so should also strongly consider the implementation of a regular window/blackout policy[25] for directors, officers, and other employees regularly exposed to inside information. A window/blackout policy would restrict covered persons to trading company securities only during open quarterly window periods (typically structured as one to three full trading days after the quarterly/annual earnings release and extending until an appropriate time before the end of the quarter). In structuring the window/blackout period, consider the times at which insiders generally are exposed to inside information, the timing of earnings release and the types of information that are truly material. The window/blackout period should be designed so that trading is prohibited during those times when insiders generally are exposed to inside information. Companies also should periodically evaluate whether their window/blackout periods apply to the right group of people. In this regard, consideration should be given to whether the window/blackout policy should apply to the assistants of those subject to the window/blackout period.
7. ***Special Blackout Periods.*** Even companies that employ regular window/blackout periods should establish procedures for calling special blackout periods during those times when unexpected material developments arise, such as the negotiation of a material acquisition or disposition. Moreover, policies should make it clear that communications regarding the existence of a special blackout period are strictly prohibited.

8. ***Rule 10b5-1 Trading Plans.*** Companies should encourage and make available to their directors and officers the ability to establish Rule 10b5-1 trading plans for trading company securities. Such plans provide directors and officers with the flexibility to trade, and, if structured correctly, an affirmative defense to an insider trading claim. To help see that such plans are structured correctly and will provide a meaningful defense, companies should consider requiring preclearance of all Rule 10b5-1 trading plans, including any modifications and cancellations. They also should consider limiting entry into such plans to open trading periods, requiring an appropriate waiting period between the establishment of a plan and the first sale thereunder (as well as between the amendment/termination of an existing plan and the entry into a new plan), limiting the number of plans and plan amendments that an insider may enter into in any given year, and requiring public disclosure of certain Rule 10b5-1 trading plans.
9. ***Hedging, Pledging and Speculative Transactions.*** Companies with insider trading policies that do not already address hedging, pledging and speculative transactions should consider revising those policies accordingly. Hedging, pledging, and speculative transactions can raise insider trading concerns and result in unnecessary negative press. In the case of pledging, because securities pledged as collateral for a loan may be sold without the consent of the pledgor upon a default, the foreclosure sale could occur at a time when the pledgor is aware of material non-public information. SEC rules already require public companies to disclose whether any shares held by their directors (and nominees) and named executive officers are pledged[26] and under the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), the SEC is required to adopt additional rules requiring companies to disclose their policies with respect to director and employee hedging of company securities.[27]
10. ***International Insider Trading Laws.*** With the pursuit of international insider trading by the SEC and the focus on insider trading violations by foreign regulators, companies with international operations and/or employees in foreign countries should not only address U.S. insider trading laws in their insider trading policies, but also the applicable insider trading laws of relevant non-U.S. countries.
11. ***Policy for Reporting Suspected Insider Trading Violations.*** Companies should confirm that directors, officers, employees, and consultants are aware of internal company policies for reporting suspected insider trading violations and find ways to strongly encourage internal reporting. Under the Dodd-Frank Act, the SEC has been authorized to pay more significant financial rewards to insider trading whistleblowers than previously authorized.[28] Given the significant incentives for directors, officers, employees, and consultants to report suspected violations to the SEC under this program, company personnel are more likely than before to be motivated to report suspected violations directly to the SEC, limiting the ability of companies to address problems internally before they are faced with an SEC investigation.
12. ***Safeguarding Information.*** Companies should undertake a review of the policies and procedures they have in place to safeguard confidential information. While an effective insider trading program will prohibit the disclosure of such information to anyone outside the company, to further protect and deter the use of such information, companies should see that they take precautions to limit access to confidential information both within and outside the company. For example, companies can use password protected files and servers for confidential information, and share the most sensitive of information only with those employees who have a need to know. Companies also should consider revising their employee handbooks or codes of conduct to

expressly prohibit employees from participating, whether for compensation or not, in expert networks. In addition, companies also should review their Regulation FD and other external communication policies to confirm that such policies adequately limit the types of information that may be disclosed outside the company and the persons authorized to disclose that information.

Conclusion

With all signs pointing toward the continued pursuit of insider trading by the SEC and other authorities, the time has come for companies to reevaluate their insider trading programs and policies. A robust program crafted in accordance with the principles described above will provide important protection for companies and their insiders.

NOTES

1. 17 C.F.R. § 240.10b-5 (2010). *See* 15 U.S.C. § 78j (2010).

2. In general, under the classical and misappropriation theories, a tipper and tippee can be held liable for insider trading if (1) the tipper discloses material non-public information in breach of a duty owed to the company's stockholders (in the case of the classical theory)/source of the information (in the case of the misappropriation theory), (2) the tippee knew or should have known of such breach, and (3) the tipper obtains a personal benefit by disclosing such information to the tippee.

3. *U.S. v. O'Hagan,* 521 U.S. 642, 651-652 (1996); *Dirks v. SEC,* 436 U.S. 646, n.14 (1983).

4. 521 U.S. 642, 652.

5. 436 U.S. 646, n.14.

6. 17 C.F.R. § 240.10b5-2(b)(2)-(3).

7. 15 U.S.C. § 78t (2010).

8. *See* Adjustment to Civil Monetary Penalty Amounts, Securities Act Release No. 9009, Exchange Act Release No. 599449, Investment Advisers Act Release No. 2845, Investment Company Act Release No. 28635, at 9 (February 25, 2009), *http://www.sec.gov/rules/final/2009/33-9009.pdf.*

9. Such liability is in addition to any disgorgement of profits that is available.

10. 15 U.S.C. § 78u-1 (2010). Registered broker-dealers and investment advisers, who have an affirmative duty under Section 15(f) of the Exchange Act and Section 204A of the Investment Advisers Act of 1940 to establish, maintain, and enforce written policies designed to prevent the misuse of non-public information, may be liable under Section 21A if they fail to establish or enforce such policies, and if that failure substantially contributes to an insider trading violation.

11. H.R. Rep. No. 100-910, at 17 (1988).

12. 15 U.S.C. § 78t(e) (2010).

13. *SEC v. Dorozhko,* 574 F.3d 42, 42-44 (2d Cir. 2009).

14. SEC Complaint, *SEC v. Dorozhko,* 2007 WL 5042904 (S.D.N.Y. filed October 29, 2007).

15. SEC Appellate Brief, *SEC v. Dorozhko,* 2008 WL 6995897 (2d Cir. filed May 12, 2008).

16. *Dorozhko,* 547 F.3d 42, 49.

17. SEC Complaint, *SEC v. Cuban,* 2008 WL 4901149, No. 3-08CV 2050-D (N.D. Tex. filed November 17, 2008); SEC Memorandum of Law in Opposition to Defendant Mark Cuban's Motion to Dismiss, 2009 WL 602920, No. 3-08-CV-2050-D (SAF) (N.D. Tex. filed February 27, 2009).

18. *SEC v. Cuban,* 620 F.3d 551, 557-558 (5th Cir. 2010).

19. Preet Bharara, U.S. Attorney for Southern District of New York, "The Future of White Collar Enforcement: A Prosecutor's View," Prepared Remarks Before the New York City Bar Association, at 5 (October 20, 2010), *http://www.nycbar.org/pdf/The%20Future%20of%20White%20Collar%20Enforcement-Prepared%20Remarks.pdf.*

20. Zachary A. Goldfarb, "Ruling Allowing Wiretaps in Some Financial Fraud Cases Could Lead to More Surveillance in Insider Trading Probes," The Washington Post (November 24, 2010), *http://www.washingtonpost.com/wp-dyn/content/article/2010/11/24/AR2010112406456.html.*

21. *See* for example, *SEC v. Benhamou*, No. 10-CV-8266 (S.D.N.Y. filed Nov. 2, 2010); Susan Pulliam *et al.,* "U.S. in Vast Insider Trading Probe," Wall St. J. (Nov. 20, 2010); Susan Pulliam,"Reluctant Analyst Pressured by the FBI," Wall St. J. (Dec. 4, 2010); *U.S. v. Dung Ching Trang Chu*, No. 1:10mj2625, (S.D.N.Y. filed Nov. 23, 2010); *U.S. v. Shimmon*, No. 1:10mj2823, (S.D.N.Y. filed Dec. 15, 2010); and *U.S. v. Jiau*, No. 10-Ωmj-02900 (S.D.N.Y. filed Dec. 23, 2010).

22. "SEC Brings Expert Network Insider Trading Charges—Moonlighting Employees Passed Company Secrets to Hedge Funds" (February 3, 2011), *http://www.sec.gov/news/press/2011/2011-38.htm.*

23. Katya Wachtel, "Another Primary Global Expert Pleads Guilty To Insider Trading," Business Insider (January 11, 2011), *http://www.businessinsider.com/expert-network-firm-emoployee-pleads-guilty-insider-trading-fbi-bob-nguyen-011-1;* Jenny Strasburg and Chad Bray, "Analyst Admits Recruiting Leakers," Wall St. J. (January 12, 2011).

24. The decision in *SEC v. Obus,* 2010 WL 3703846 (S.D.N.Y 2010), highlights the importance of obtaining express confidentiality

agreements from third parties who may have access to inside information as such agreements may provide persuasive evidence of the existence of a "special relationship" necessary to establish "temporary insider" status.

25. Some companies refer to this as a "quiet period."

26. *See* Item 403(b) of Regulation S-K.

27. Dodd-Frank Wall Street Reform and Consumer Protection Act § 955.

28. Prior to the law's adoption, the bounty program only applied to insider trading cases and capped whistleblower awards at 10% of the penalties collected in the action.