MORRISON | FOERSTER

Legal Updates & News

Legal Updates

Courts Push Back on SEC's Pursuit of Insider Trading by Non-Fiduciaries

July 2009
by Mia Mazza, Marisa Lopez McDonald

Related Practices:

- Corporate Litigation
- Public Companies & Corporate Governance
- Securities Litigation, Enforcement and White-Collar Defense

Two recent cases reflect the efforts of the U.S. Securities and Exchange Commission to expand the scope of insider trading law — and courts' pushing back against those efforts. These decisions underscore the need for companies wishing to prevent inappropriate trading to go beyond nondisclosure agreements with outsiders who are entrusted with sensitive information.

In *SEC v. Cuban*, Civ. Act. No. 3:08-CV-2050-D (N.D. Tex. July 17, 2009), the defendant (Mark Cuban, a non-insider) was provided with material nonpublic information after entering into a confidentiality agreement with the source company. He otherwise had no pre-existing fiduciary relationship with the company and did not make an agreement to refrain from using the information for his own benefit. After he traded on the information, the Securities and Exchange Commission brought an enforcement action under the "misappropriation" theory of insider trading. The court dismissed the complaint, finding that Cuban's trading did not violate the federal securities laws. Rejecting SEC Rule 10b5-2 and arguably departing from prior decisions, the court held that Cuban's agreement not to *disclose* the confidential information did not give rise to a duty to refrain from *using* the information.

The Texas court's ruling was especially notable in light of an alleged telephone conversation between Cuban and the company's CEO. After hearing the confidential information, Cuban stated, "Well, now I'm screwed. I can't sell." The court ruled that this statement "cannot reasonably be understood as an agreement not to sell." The CEO's unilateral expectation that Cuban's statement meant he would not trade on the information was irrelevant.

Last week, another SEC enforcement complaint was dismissed, this time by the Second Circuit in *SEC v. Dorozhko*, No. 08-0201-cv (2d Cir. July 22, 2009). There, the defendant traded on material nonpublic information he had obtained by "hacking" into the computer system of a vendor of the source company. The SEC's complaint asserted that computer hacking is "deceptive" and thus the hacker's trading violated the federal securities laws. The defendant moved to dismiss, arguing that the SEC could not

prevail on this theory without demonstrating a fiduciary relationship between the hacker and the source company (which the SEC conceded did not exist). The district court agreed.

The appellate court agreed that, without a fiduciary duty to refrain from trading, the mere act of trading on information obtained by "hacking" did not violate the securities laws. The court gave the SEC a chance to amend its complaint, however, to provide more information about the specific nature of this hacker's activity. If he merely exploited a weakness in the vendor's computer system, there was no violation. But if, for example, the hacker gained access to the information by falsely identifying himself as another user, that could be considered an affirmative misrepresentation ("a distinct species of fraud"), and the SEC could go forward even without a fiduciary duty.

It remains to be seen whether the SEC appeals the *Cuban* decision or is successful in repleading *Dorozhko*. It also remains to be seen whether the courts push back even further and begin questioning whether the SEC has exceeded its interpretive authority in other ways.

For now, these decisions demonstrate the need for companies wishing to prevent inappropriate trading to take special care to protect inside information. Confidentiality agreements with vendors, employees, and other outsiders should be updated to provide explicitly that the recipient of the confidential information will not only refrain from disclosing the information, but also will refrain from using it for his or her own benefit. These developments also highlight the importance of ensuring that vendors and others to whom you entrust sensitive information are maintaining robust data security mechanisms.
