New York Law Journal
Corporate Update
WWW.NYLJ.COM

An incisivemedia publication
VOLUME 242—NO. 46
THURSDAY, SEPTEMBER 3, 2009

CORPORATE CRIME

'Outsiders' as 'Insiders': Recent Insider Trading Cases

Generally, corporate "outsiders"—persons with no direct or derivative fiduciary duty to a corporation or its shareholders—have been held liable for insider trading only when they had a fiduciary or fiduciary-like relationship with the source of the material, non-public information on which they traded. After a period of controversy and uncertainty, the Supreme Court, in *United States v. O'Hagan*,[1] adopted the so-called "misappropriation" theory and thereby appeared to make clear the circumstances in which a corporate outsider would be liable. In *O'Hagan*, the Court held "that a person commits fraud 'in connection with' a securities transaction, and thereby violates §10(b) and Rule 10b-5, when he misappropriates confidential information for securities trading purposes, in breach of a duty owed to the source of the information."[2]

Two recent cases—a district court decision from the Western District of Texas and a Second Circuit decision—illustrate that the precise contours of the misappropriation theory are still uncertain and the subject of continuing judicial development.

By
Howard W. Goldstein

'SEC v. Cuban'

In *SEC v. Cuban*,[3] the SEC brought civil insider trading charges against Mark Cuban—the owner of the Dallas Mavericks NBA team—based on the misappropriation theory. The SEC alleged that Cuban, who owned 6.3 percent of the stock of a company called Mamma.com, first agreed to keep confidential material, non-public information that Mamma.com planned a private investment in public equity (PIPE) transaction, and then traded based on that information to avoid expected losses when the PIPE was publicly announced. The issue before the court was whether, absent a pre-existing fiduciary or fiduciary-like duty, a confidentiality agreement created a duty sufficient to support application of the misappropriation theory.

Turning to *O'Hagan*, Chief Judge Fitzwater noted that "'[d]eception through nondisclosure is central to [this] theory[.]'" and that "deception inheres in the undisclosed use of information in breach of a duty not to do so."[4] Although urged in an amicus brief by five law professors to reject the argument that a confidentiality agreement was sufficient to create a fiduciary or similar relationship of trust and confidence,[5] the court concluded that there was "no apparent reason why that duty cannot arise by agreement."[6] The court, however, rejected the SEC's claims, holding that there was a distinction between an agreement not to disclose information and an agreement not to trade on the information or otherwise use it for personal gain. Because Cuban had only agreed not to disclose the information he had been given, Cuban's use of the information did not breach any duty, and he was not liable under Section 10(b).

'Dorozhko'—The District Court

In *SEC v. Dorozhko*,[7] the SEC brought an action for a preliminary injunction, seeking to freeze the proceeds of the defendant's extremely profitable trading in put options of IMS Health Inc. ("IMS"). The SEC alleged that Dorozhko hacked into the computer network of a company that hosted the IMS investor relations Web site and obtained a yet to be released negative earnings announcement, after which he traded on that information and realized an overnight profit of $286,000, or 697 percent of his investment. Dorozhko asserted his Fifth Amendment privilege during the district court proceedings. After the preliminary injunction hearing, Judge Buchwald asked both parties to address "the question whether the alleged 'stealing and trading' or 'hacking and trading' constitutes a violation of §10(b) and Rule 10b-5."[8]

In resolving this question, Judge Buchwald started from the non-controversial premise that a Rule 10b-5 violation required "(1) a 'device or contrivance'; (2) which is 'manipulative or deceptive'; and (3) used 'in connection with' the purchase or sale of securities."[9] She quickly concluded that requirements (1) and (3) were satisfied and, citing *Santa Fe Indus. v. Green*,[10] that hacking was not manipulative within the established meaning of the securities laws. The determinative question, therefore, was whether Dorozhko's alleged hacking was deceptive.

The balance of the district court's opinion—described by the Second Circuit as "thoughtful and careful"—was devoted to answering that question. Judge Buchwald reviewed in detail the historical progression of insider trading cases, as well as the legal academic literature. Noting that in the 74 years since its passage, no federal court had ever held that theft of material, inside information by a corporate outsider could be a basis for a violation of Section 10(b), the Court stated that "[a]lthough the case law could very well have developed differently, see *Chiarella* [445 U.S. 222, 246 (Blackmun, J. dissenting)], and there are respectable arguments that it should have developed differently, a breach of a fiduciary duty of disclosure is a required element of any 'deceptive' device under §10(b)."[11] The court, therefore, was constrained to hold that Dorozhko's alleged "stealing and trading" or "hacking and trading" does not amount to a violation of §10(b) and Rule 10b-5 because Dorozhko did not breach any fiduciary or similar duty…. Although Dorozhko may have broken the law, he is not liable in a civil action under §10(b) because he owed no fiduciary or similar duty either to the source of his information or to those he transacted with in the market.[12]

Two additional observations by the District Court are worthy of note. First, Judge Buchwald noted that while both hacking and traditional theft may involve

---

HOWARD W. GOLDSTEIN *is a partner at Fried, Frank, Harris, Shriver & Jacobson.* JOHNATHAN J. SMITH*, an associate at the firm, assisted in the preparation of this article.*

deception "in the common law sense of unauthorized access," they do not involve "deception in the sense of a breach of a duty of disclosure."[13] Second, Judge Buchwald observed that "[t]his case highlights a potential gap arising from reliance on fiduciary principles in the legal analysis that courts have employed to define insider trading…."[14] That gap was reflected in the views of the legal academics cited by the District Court, who for the most part concluded that hackers should be liable but, as thieves, are not liable under current law for insider trading.[15]

'Dorozhko'—Second Circuit

On appeal, the Second Circuit framed the issue before it as follows:

> We are asked to consider whether, in a civil enforcement lawsuit brought by the United States Securities and Exchange Commission ("SEC") under Section 10(b) of the Securities Exchange Act of 1934 ("Section 10(b)"), computer hacking may be "deceptive" where the hacker did not breach a fiduciary duty in fraudulently obtaining material, nonpublic information used in connection with the purchase or sale of securities.[16]

In answering that question, the court started with the SEC's concession that its case was "not based on either of the two generally accepted theories of insider trading"—the traditional theory involving trades by corporate insiders, or the misappropriation theory involving trades by corporate outsiders who breach a fiduciary duty owed to the source of their information.[17] The court then analyzed the principal cases the District Court had relied upon in concluding that deception required a breach of a fiduciary duty—*Chiarella v. United States*,[18] *United States v. O'Hagan*,[19] and *SEC v. Zandford*.[20] From its review, the court concluded that those cases—individually or collectively—did not establish that breach of a fiduciary duty was a necessary element of every Section 10(b) violation, because in each of those cases, "the theory of fraud was silence or non-disclosure, not an affirmative misrepresentation."[21] As to the SEC's affirmative misrepresentation theory in the *Dorozhko* case, the Court stated it was "aware of no precedent of the Supreme Court or our Court that forecloses or prohibits the SEC's straightforward theory of fraud" and that "[a]bsent a controlling precedent that 'deceptive' has a more limited meaning than its ordinary meaning, we see no reason to complicate the enforcement of Section 10(b) by divining new requirements."[22]

That, of course, left the question whether Dorozhko's hacking had been accomplished by means of an "affirmative misrepresentation." And on that question, the court understandably punted. Because the District Court's analysis had not required it to address the question whether Dorozhko's hacking had involved any misrepresentation, the court simply vacated the District Court's order and remanded for further proceedings.

Some Thoughts

The Second Circuit relied heavily on dictionary definitions of the word "deceptive" in reaching its conclusion that "[i]n its ordinary meaning, 'deceptive' covers a wide spectrum of conduct involving cheating or trading in falsehoods."[23] The Court went on to note that "[i]n light of this ordinary meaning, it is not at all surprising that Rule 10b-5 equates 'deceit' with 'fraud.'"[24] But the language of rule 10b-5 then quoted by the Court refers to conduct that would operate as a fraud or deceit upon any "person." And whatever dictionary definitions one uses, and whatever one's views on artificial intelligence, there is no legal support for the notion that a computer can be a defrauded "person" for purposes of the securities laws.

On the other hand, there is legal support for the conclusion that, in some circumstances, a theft can be a fraud. Thus, in *United States v. Finnerty*,[25] the district court noted that "[a]s the Supreme Court has made clear…theft by itself does not constitute securities fraud because of the requirement of deception [citing *Zandford*]," but that "theft constitutes fraud only when it is accompanied by a violation of fiduciary duty." And, in *Horn's Inc. v. IM International Publishing Inc.*,[26] a case that arose in a fiduciary duty employer-employee context, the court stated that the theft of confidential information could be mail fraud if there were an intent to defraud "either by affirmative misrepresentations or by silence."

It seems the situation of a hacker gaining access to insider information and trading on it is a case in which technology has outstripped the securities laws. But in that situation, and in the case of theft generally, the remedy—if securities laws enforcement is deemed appropriate—is for Congress to amend the securities laws, rather than to require district courts and lawyers to untangle the nature of hacking and other forms of theft, on a case-by-case basis, in search of an affirmative misrepresentation.

To distinguish between theft and fraud in the case of hacking into a computer, the Second Circuit focused on affirmative misrepresentation. But what is an affirmative misrepresentation in the case of "tricking" a computer? And more generally, query whether reliance on an affirmative misrepresentation makes sense as a basis for determining the difference between theft and fraud for the purpose of enforcing the securities laws. Under the Second Circuit's opinion in *Dorozhko*, a law firm client who is on the premises of a law firm for a legitimate purpose and who sees information about a tender offer on an open computer and trades on it may be a thief, but he is not liable for securities fraud. On the other hand, a thief who steals a lawyer's wallet, uses his card key to gain access to the law firm's premises, sees information on an open computer, and then trades on that information, has arguably misrepresented his identity to gain access and is liable for securities fraud, even though no person has been defrauded. But what if the thief is legitimately on the law firm's premises delivering lunch to a conference room and, while on the premises, picks the lock on an office to obtain confidential information? Is that "deceiving the lock" (fraud), or is it exploiting a security weakness (theft)?

As Judge Buchwald noted, there are ample criminal penalties available outside the securities laws to punish hackers who steal and trade. It seems the situation of a hacker gaining access to insider information and trading on it is a case in which technology has outstripped the securities laws. But in that situation, and in the case of theft generally, the remedy—if securities laws enforcement is deemed appropriate—is for Congress to amend the securities laws, rather than to require district courts and lawyers to untangle the nature of hacking and other forms of theft, on a case-by-case basis, in search of an affirmative misrepresentation.

1. 521 U.S. 642 (1997).
2. Id. at 652.
3. No. 3:08-cv-2050 (SAF), 2009 U.S. Dist. LEXIS 61574 (N.D. Tex. July 17, 2009).
4. Id. at *21 (quoting *O'Hagan*, 521 U.S. at 654).
5. Brief of Stephen Bainbridge et al. as Amici Curiae in Support of Defendant's Motion to Dismiss, *SEC v. Cuban*, 2009 U.S. Dist. LEXIS 61574.
6. 2009 U.S. Dist. LEXIS 61574, at *23. See also *SEC v. Yun*, 327 F.3d 1263, 1273 (11th Cir. 2003) (acknowledging that "a breach of an agreement to maintain business confidences would also suffice" to yield insider trading liability); *SEC v. Nothern*, 598 F.Supp.2d 167, 175 (D. Mass. 2009) ("a contract providing a corporate outsider access to confidential information may be sufficient to create a duty from which misappropriation liability may arise.").
7. 606 F.Supp.2d 321 (S.D.N.Y. 2008), vacated and remanded, No. 08-0201-cv, 2009 U.S. App. LEXIS 16057 (2d Cir. July 22, 2009).
8. Id. at 327.
9. Id. at 328.
10. 430 U.S. 462, 473 (1977).
11. 606 F.Supp.2d at 330.
12. Id. at 324 (citation omitted).
13. Id. at 339.
14. Id. at 323.
15. Id. at 341-2.
16. 2009 U.S. App. LEXIS 16057, at *2.
17. 2009 U.S. App. LEXIS 16057, at *6 (citation omitted).
18. 445 U.S. 222 (1980).
19. 521 U.S. 642 (1997).
20. 535 U.S. 813 (2002).
21. 2009 U.S. App. LEXIS 16057, at *16.
22. Id. at *19.
23. Id. at *22 (citations omitted).
24. Id. at *23 (citing 17 C.F.R. §240.10b-5 (2009)).
25. 474 F.Supp.2d 530, 543 (S.D.N.Y. 2007).
26. No. 85 Civ. 8853 (WCC), 1986 U.S. Dist. LEXIS 19255, *9 (S.D.N.Y. Oct. 9, 1986).