Second Circuit Rules Computer Hacking May Be "Deceptive" Under Section 10(b) of the Securities Exchange Act of 1934

STEWART D. AARON, MARCUS ASNER, AND YUE-HAN CHOW

This article discusses a recent Second Circuit decision which permits the U.S. Securities and Exchange Commission to pursue cases of computer hacking as violations of the federal securities laws in circumstances where they also could be prosecuted as violations of the various federal criminal fraud statutes.

In a recent decision, the U.S. Court of Appeals for the Second Circuit held that a computer hacker who accesses a company's nonpublic securities information and then trades on that information can be found liable for violating the federal securities laws, even in a situation where a hacker did not owe or breach a fiduciary duty. The court in *SEC v. Dorozhko,*[1] held that, in order to establish liability under Section 10(b) of the Securities Exchange Act of 1934, the U.S. Securities and Exchange Commission ("SEC") did not need to establish that the hacker owed and breached a fiduciary duty in a case where the hacking activity itself constitutes a fraudulent misrepresentation, in contrast to a fraudulent nondisclosure.

Typically, claims alleging that someone has engaged in securities

Stewart D. Aaron is a partner practicing securities and commercial litigation in Arnold & Porter LLP's New York office, where he also serves as the administrative partner. Marcus Asner is a partner at the firm in the white collar criminal defense practice group. Yue-Han Chow is an associate at the firm and a member of the litigation practice group. The authors may be contacted at stewart.aaron@aporter.com, marcus.asner@aporter.com, and yue-han.chow@aporter.com, respectively.

Published in the October 2009 issue of Privacy & Data Security Law Journal.

fraud, such as insider trading, require a showing that the person owed a fiduciary duty to disclose his or her access to nonpublic information. A hacker who is a stranger to the company but who nevertheless manages to access nonpublic securities information typically owes no such duty and cannot be held liable for nondisclosure under the securities laws; instead, this sort of hacking activity may be prosecuted as a computer intrusion or even as an outright theft. However, the Second Circuit in *Dorozhko* recognized that computer hacking can involve an affirmative misrepresentation as part of a scheme to gain access to nonpublic information (the hacker can lie about her identity to gain access, for example), and that such a misrepresentation would qualify as a deceptive device under Section 10(b) of the Securities Exchange Act of 1934. The *Dorozhko* decision makes clear that the SEC may investigate and regulate certain activities in cyberspace which more commonly are the subject of prosecution under federal criminal statutes, such as the computer fraud statute, 18 U.S.C. § 1030.

THE SECOND CIRCUIT'S OPINION

In *SEC v. Dorozhko*, the SEC sought a preliminary injunction in an enforcement action to freeze the proceeds of trades by a Ukrainian national who had hacked into a financial information service company's computer network to obtain nonpublic information, which he then used to buy "put" options of a company's stock. IMS Health Inc. ("IMS") announced it would release its third quarter earnings during a conference call on a certain date after the market closed and engaged Thomson Financial, Inc. ("Thomson") to manage the online release of the earnings report. The day before the earnings call, Dorozhko successfully hacked into Thomson's computer system and downloaded information on IMS. Soon afterwards, he used an online trading account to purchase 90 percent of all put options for IMS stock for the six weeks before the earnings call, betting that the company's stock price would decrease significantly within a short amount of time. The day after the earnings report announcement, IMS's stock price sank, and Dorozhko sold all of his IMS options within six minutes of the market opening, realizing a profit of $286,456.59.

The company that serviced Dorozhko's online trading account noticed

the irregular trading activity and referred the case to the SEC. After obtaining a temporary restraining order to freeze the proceeds of Dorozhko's brokerage account from the U.S. District Court for the Southern District of New York, the SEC then sought a preliminary injunction. The district court denied this request.[2] It concluded that the U.S. Supreme Court in three cases — *Chiarella v. United States*,[3] *United States v. O'Hagan*,[4] and *SEC v. Zandford*[5] — required that there be a breach of fiduciary duty to disclose or abstain in order for there to be a deceptive device in violation of Section 10(b).[6] Accordingly, the district court held that, in the absence of any showing that the defendant owed a fiduciary duty to disclose his use of non-public information to trade securities, the SEC's request for a preliminary injunction must be denied because it had not shown a likelihood of succeeding on the merits of its claim.[7]

On appeal, the Second Circuit examined the three Supreme Court cases on which the district court based its holding that a fiduciary relationship was required to make the defendant's silence actionable under Section 10(b). The first case, *Chiarella*, held that for a plaintiff to establish that a defendant committed fraud due to a nondisclosure under Section 10(b), the plaintiff necessarily had to show that the defendant had a duty to speak. *Chiarella* involved an employee at a financial printer who used information from the corporate takeover bids that his employer was printing to purchase stock in the target companies and to sell the stock after news of the attempted takeovers were made public. The Supreme Court noted that under the traditional theory of insider trading, "silence in connection with the purchase or sale of securities may operate as a fraud actionable under § 10(b)…But such liability is premised upon a duty to disclose arising from a relationship of trust and confidence between parties to a transaction."[8] Based on this rule, the Supreme Court held that "there can be no fraud [based on nondisclosure] absent a duty to speak" and that the duty to disclose "does not arise from the mere possession of nonpublic market information."[9]

The second case cited by the district court in *Dorozhko*, *O'Hagan*, picked up where *Chiarella* left off — that is, it addressed the misappropriation theory of liability.[10] In *O'Hagan*, the defendant was a partner in a law firm who used nonpublic information he acquired through his firm's

Published in the October 2009 issue of Privacy & Data Security Law Journal.

representation of a client in order to trade securities. The Supreme Court held that "a misappropriator who trades on the basis of material, nonpublic information, in short, gains his advantageous market position through deception; he deceives the source of the information and simultaneously harms members of the investing public."[11]

The last case relied upon by the district court, *Zandford*, applied the misappropriation theory of liability to an instance of outright theft by a broker from his client. In *Zandford*, a broker used a client's investment account to buy and sell securities and pocketed the proceeds. The defendant was first indicted on wire fraud charges, and the SEC followed with a civil suit, alleging that the defendant violated Section 10(b) and Rule 10b-5 by engaging in a scheme to defraud his client and misappropriating his client's securities.[12] The issue was whether the defendant's fraud could be considered "in connection with" the sale of a security; the U.S. Court of Appeals for the Fourth Circuit had held that it could not because, to do so, the court would have to "stretch the language of the securities fraud provisions to encompass every conversion or theft that happens to involve securities."[13] The Supreme Court reversed on the ground that, because the complaint described "a fraudulent scheme in which the securities transactions and breaches of fiduciary duty coincide," the requirement that the breaches be "in connection with" securities sales under Section 10(b) had been met.[14]

The Second Circuit in *Dorozhko* distinguished the three Supreme Court cases relied upon by the district court by noting that they only dealt with instances in which the defendants allegedly violated Section 10(b) because they stayed silent when using material, nonpublic information in connection with the sale of securities. In contrast, the defendant in *Dorozhko* — by hacking into a computer system to gain access to nonpublic information — may well have made an affirmative misrepresentation along the way. The court observed that the hacking may well have involved "employ[ing] electronic means to trick, circumvent, or bypass computer security in order to gain unauthorized access to computer systems, networks, and information…and to steal such data." Similarly, Dorozhko may have misrepresented his identity to gain access to secured information. The court reasoned that if the hacking involved making an affirmative misrepresentation, it would be a "deceptive device" under Section

10(b) and Rule 10b-5 "rather than being mere theft." The court noted that the Supreme Court did not require a fiduciary relationship as an element of every actionable securities claim under Section 10(b). The Second Circuit therefore vacated and remanded the case to the district court to consider whether the particular method of computer hacking that Dorozhko used involved a fraudulent misrepresentation, which would not require a showing that the defendant owed a fiduciary duty to anyone, or whether his method of hacking was more akin to a simple, non-fraudulent theft.

IMPLICATIONS OF THE DECISION

The Second Circuit's decision in *Dorozhko* permits the SEC to pursue cases of computer hacking as violations of the federal securities laws in circumstances where they also could be prosecuted as violations of the various federal criminal fraud statutes, such as the wire fraud statute.[15] Indeed, both the district court and the Second Circuit noted that such "hacking and trading" schemes have typically been prosecuted under federal and/or state criminal statutes.[16] This decision provides the SEC wide latitude in determining how to address securities-related misconduct. Given the prosecutorial burdens on and priorities of the U.S. Department of Justice, such latitude is to be expected.

NOTES

1 *SEC v. Dorozhko*, No. 08-0201-CV (July 22, 2009).
2 *SEC v. Dorozhko*, 606 F. Supp. 2d 321 (S.D.N.Y. 2008).
3 *Chiarella v. United States*, 445 U.S. 222 (1980).
4 *United States v. O'Hagan*, 521 U.S. 642 (1997).
5 *SEC v. Zandford*, 535 U.S. 813 (2002).
6 606 F. Supp. 2d at 338-39.
7 *Id.* at 343.
8 445 U.S. at 230.
9 *Id.* at 235.
10 521 U.S. at 662.
11 *Id.* at 656.
12 535 U.S. at 816.

[13] *Id.* at 817-18.

[14] *Id.* at 825.

[15] The federal wire fraud statute reads:

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both. If the violation affects a financial institution, such person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both. 18 U.S.C. § 1343.

To sustain a conviction under this statute, the government must prove that there was (1) a scheme to defraud; and (2) use of wire communications in furtherance of the scheme. *See, e.g., United States v. Riggs*, 739 F. Supp. 414 (N.D. Ill. 1990) (computer hacker charged under the federal wire fraud statute).

[16] 606 F. Supp. 2d at 323, 324.

Published in the October 2009 issue of Privacy & Data Security Law Journal.