

SECOND CIRCUIT TO COMPUTER HACKERS: INSIDER TRADING LAWS APPLY

August 14, 2009

To Our Clients and Friends:

On July 22, 2009, the United States Court of Appeals for the Second Circuit (the “Court”) vacated a district court’s conclusion that computer hacking to obtain material non-public information about an issuer of publicly-traded securities cannot be “deceptive” for purposes of establishing insider trading liability unless the conduct involved a breach of a fiduciary duty. The Court’s decision is worth noting for two primary reasons. First, the decision potentially strengthens the SEC’s ability to combat insider trading by making clear that a fiduciary-duty requirement is not an element of every violation of Section 10(b) that involves a “deceptive device.” Second, the decision establishes that computer hacking may serve as the basis for an insider trading action if the means used to gain the unauthorized computer access involved an affirmative misrepresentation or deception.

The case stems from a computer hacker gaining access to a computer server housing a registrant’s earnings report prior to its release and then profiting from the information in that report through the purchase and sale of the registrant’s securities. Interestingly, neither the SEC’s original claim against the defendant nor its appeal to the Court was based on either of the two generally accepted theories of insider trading (*i.e.*, the “traditional theory,” in which a corporate insider trades on material, non-public information, and “misappropriation theory,” in which a person trades on material, non-public information that has been gained in violation of a fiduciary or other identifiable duty). A key element of each of these theories is the existence and breach of a fiduciary or other identifiable duty to the source of the insider information, and the defendant in the case was not a corporate insider and did not owe any duty to the registrant or the owner of the computer system that was hacked. Instead, the SEC utilized a straightforward fraud theory claiming that the defendant affirmatively misrepresented himself in order to gain access to material, non-public information, which he then used to trade. As such, the SEC contended that the defendant’s computer hacking constituted a “deceptive device” in violation of Section 10(b) and Rule 10b-5.

In the original action, the district court dismissed the SEC’s claims and ruled that computer hacking was not “deceptive” within the meaning of Section 10(b), absent a breach of a fiduciary duty. In support of its conclusion, the district court determined that Supreme Court jurisprudence on the issue interpreted the “deceptive” element of Section 10(b) to require a breach of a fiduciary duty generally. Following a brief review of the principal

Supreme Court cases upon which the district court relied (*Chiarella v. United States*, *United States v. O'Hagan* and *SEC v. Zandford*), the Court disagreed with the district court's analysis (which it termed "thoughtful and careful") and concluded that none of those cases imposed a fiduciary duty requirement where the deception alleged involved an affirmative misrepresentation, rather than mere non-disclosure. While agreeing that non-disclosure is actionable only where there is a duty to speak, the Court concluded that no such duty is required in the case of an affirmative misrepresentation. In reaching its conclusions, the Court emphasized the need to construe Section 10(b) "flexibly to effectuate its remedial purposes."

The Court then turned to the following question not considered by the district court: whether the ordinary (*i.e.*, dictionary) meaning of "deceptive" covers computer hacking or whether the defendant's computer hacking actually involved an affirmative misrepresentation. The Court concluded that, depending upon the method of access used by a computer hacker, computer hacking could be "by definition, a 'deceptive device or contrivance' that is prohibited by Section 10(b) and Rule 10b-5." The Court then remanded the case to the district court to consider whether the defendant's computer hacking constituted such a "deceptive device or contrivance." Drawing from the Court's decision, if the defendant misrepresented his identity in hacking the computer server to gain access to the registrant's earnings release, such a misrepresentation would render the hacking actionable under Section 10(b) and Rule 10b-5. Less clear from the Court's decision is whether other means used to gain unauthorized entry (*e.g.*, exploiting a weakness in an electronic code) would render the hacking actionable under Section 10(b) and Rule 10b-5.

* * * *

While the Court's conclusion that a "deceptive device" does not require a breach of fiduciary duty to fall within the scope of the insider trading laws (including the Court's consideration of the ordinary meaning of "deceptive") could strengthen the SEC's insider trading toolbox, it may be at odds with a recent decision rendered by the Fifth Circuit Court of Appeals (*Regents of the Univ. of Cal. U. Credit Suisse First Boston (USA), Inc.*). In any case, it will be interesting to see where the courts draw the line between criminal theft and insider trading.

Please do not hesitate to call us to discuss the Court's decision in this matter or any of the issues raised by this memorandum generally.

Matthew E. Kaplan	Paul R. Berger	Steven J. Slutzky	Colby A. Smith
+1 212 909 7334	+1 202 383 8090	+1 212 909 6036	+1 202 383 8095
mekaplan@debevoise.com	prberger@debevoise.com	sjslutzky@debevoise.com	casmith@debevoise.com