Westlaw Journal
WHITE-COLLAR CRIME
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 30, ISSUE 2 / NOVEMBER 2015

EXPERT ANALYSIS

Computer Hacking and Insider Trading Liability

By Robert A. Horowitz, Esq., and Geoffrey S. Berman, Esq.
Greenberg Traurig

The Justice Department filed criminal complaints in early August in the U.S. District Courts for New Jersey and the Eastern District of New York against several computer hackers and traders. The complaints allege violations of a host of federal anti-fraud statutes, including Sections 10(b) and Rule 10b-5 of the Securities Exchange Act of 1934.[1]

Days later the U.S. Securities and Exchange Commission filed a civil action in U.S. District Court for New Jersey against the same defendants and several others, alleging violations of Section 17(a) of the Securities Act of 1933 and Section 10(b) and Rule 10b-5 of the Exchange Act.[2]

The cases accuse "hacker defendants" of hacking into U.S. newswire services to gain access to pending press releases of publicly held companies and then selling the stolen information to "trading defendants" who allegedly acted on the stolen information.

This commentary explores whether the computer hacking and trading alleged in the complaints constitute illegal insider trading under the securities laws.[3]

Insider trading violates Section 10(b) and Rule 10b-5 of the Exchange Act only if it involves the use of a "manipulative or deceptive device in connection with the purchase or sale of securities." The Supreme Court has recognized two theories of insider trading, both of which are premised on the trader's duty either to disclose the material nonpublic information or abstain from trading.

The "classical theory" of insider trading involves a corporate insider who deceives by trading in the company's securities on the basis of material nonpublic information about the company, breaching his duty of trust and confidence owed to the company's shareholders.

The "misappropriation theory" involves a company outsider who deceives by obtaining material nonpublic information about a company from the owner of the information and then trades on the information, breaching his duty of trust and confidence owed to the source of the information.

Computer hacking cases do not fit neatly into either category because hackers owe no duty of trust and confidence to the companies and newswires victimized by their actions..

However, in *SEC v. Dorozhko,* 574 F.3d 42 (2009), the 2nd U.S. Circuit Court of Appeals expanded liability for insider trading beyond the types of actions previously outlined by the Supreme Court. It held that a computer hacker who stole material nonpublic information and then traded on the information may be liable under the securities laws if he made an affirmative misrepresentation to obtain the information.[4]

The "hacker defendants" hacked into U.S. newswire services to gain access to press releases before they were issued and sold the stolen information to the "trading defendants."

In *Dorozhko* the U.S. District Court for the Southern District of New York dismissed the SEC's complaint. Relying on *Chiarella v. United States,* 445 U.S. 222 (1980); *United States v. O'Hagan*, 521 U.S. 642 (1997); and *SEC v. Zanford*, 535 U.S. 813 (2002), the District Court concluded that in the absence of a fiduciary duty or similar duty owed to the source of the information or the counterparties to his trades, there can be no violation of Section 10b or Rule 10b-5.

The 2nd Circuit disagreed. It framed the question as "whether the 'device' in this case — computer hacking — could be 'deceptive'" within the meaning of Section 10(b) and Rule10b-5. The appeals court analyzed the Supreme Court decisions in *Chiarella, O'Hagan* and *Zanford*, and it observed that none of them unconditionally require a breach of a duty of trust and confidence as an element of insider trading.

In *Chiarella* the Supreme Court held that the defendant's nondisclosure was not fraud because he had no agency or other fiduciary relationship with the sellers of the securities he was purchasing such that he would have an obligation to disclose the information or abstain from trading. The court explained, "When an allegation is based upon nondisclosure, there can be no fraud absent a duty to speak. We hold that a duty to disclose under Section 10(b) does not arise from the mere possession of nonpublic market information."[5]

In *O'Hagan* the Supreme Court upheld the conviction of the defendant, an attorney, who traded in securities based upon material nonpublic information regarding his firm's clients because he owed a duty of trust and confidence to the source of the information to disclose that he would trade on it.

Similarly, in *Zanford* the high court held that a broker's theft of trading proceeds from his clients' accounts violated Section 10(b) and Rule 10b-5 because the broker failed to disclose to his clients, to whom he owed a fiduciary duty, that he was stealing assets from their accounts.

In *Dorozhko* the 2nd Circuit concluded that while a breach of a duty of trust and confidence is required when the deception is based on silence or nondisclosure, a duty of trust and confidence is not required in all cases.

The court noted that the SEC's insider trading claim against Oleksandr Dorozhko was not based on his silence in the face of a duty to disclose. Instead, it was based on alleged misrepresentations the defendant hacker made to gain access to the information. Thus, the court held that computer hacking could be a deceptive device or contrivance prohibited by Section 10(b) and Rule 10b-5 "depending on how the hacker gained access."

"[M]isrepresenting one's identity in order to gain access to information that is otherwise off limits, and then stealing that information is plainly 'deceptive' within the ordinary meaning of the word," but "exploiting a weakness in an electronic code to gain unauthorized access" may be "mere theft" as opposed to insider trading, the appeals court wrote.[6]

The indictments in the current hacking cases say the hackers used several methods to break into the newswires' computer systems, some of which involved affirmative misrepresentations (misrepresenting their identities by using login credentials to gain unauthorized access) and others that involved use of a computer programming language to hack into computers connected to the Internet.[7]

Thus, the allegations appear to address the two methods of computer hacking the Court of Appeals distinguished in *Dorozhko*: the use of affirmative misrepresentations to gain access (which the *Dorozhko* court held would constitute a deceptive device) and the use of software to gain access (which the *Dorozhko* court indicated might not constitute a deceptive device).

However, the current cases involve an additional wrinkle not considered by the court in *Dorozhko*. In *Dorozhko* the computer hacker traded on the information. Here, the government alleges that, after stealing the information, some of the hacker defendants did not trade but instead sold the information to the trading defendants, who in turn used it to trade. In essence, the hacker defendants who accessed the information are alleged to have tipped the trading defendants.[8]

For tipping liability to attach in a classic insider trading or misappropriation case, the tipper must breach his duty of trust and confidence owed to the source of the information, which requires a finding that the tipper not only disclosed the information but also derived a personal benefit from disclosing the information.[9]

For a tippee in those cases to be liable for insider trading, the tippee must have been aware both that the tipper disclosed the information in breach of the tipper's duty of trust and confidence and that the tipper derived a personal benefit from his or her disclosure.[10]

As discussed above, hacking cases do not fit squarely within the classical or misappropriation theories of insider trading. How tipper/tippee liability will be determined in these cases is an open question. Specifically, under *Dhorozhko*, what does the government have to prove to convict the hacker defendant tippers and the trading defendant tippees of insider trading?

CONCLUSION

These cases test the reach of federal securities laws and the scope of insider trading liability. *Dorozhko* expanded the reach to include computer hackers who traded on the information, but it did not address tipper/tippee liability in the context of computer hacking. Extending the reasoning of *Dhorozhko* to the existing tipper liability standards under *Dirks* is straightforward. Specifically, the liability of the hacker defendants would be determined based upon whether they made affirmative misrepresentations to hack into the computers to obtain the press releases and whether they personally benefited by tipping the information to the trading defendants.

The intersection of *Dorozhko* and *Newman* to establish tippee liability seems more problematic for the government. If the reasoning of *Newman* (that a tippee's liability is premised on his knowledge both that the tipper breached a duty of trust and confidence and derived a personal benefit) is applied, *Dorozhko* would appear to require the government to prove that the trading defendants knew the hacker defendants made affirmative misrepresentations to obtain the material nonpublic information.

In other words, if the current state of 2nd Circuit law is extended to tipper/tippee cases like the ones at issue here (where the tipper is a hacker who stole the tipped information through hacking), the government will have to carry the heavy burden of proving that the trading defendants were aware of the specific technology or methods the hacker defendants used to obtain that information.

*The 2nd Circuit held in Dorozhko **that computer hacking could be a deceptive device or contrivance prohibited by Section 10(b) and Rule 10b-5 "depending on how the hacker gained access."***

NOTES

[1] *United States v. Turchynov et al.*, No. 2:15-cr-00390-MCA, *indictment filed,* 2015 WL 4764144 (D.N.J. Aug. 5, 2015); *United States v. Korchevsky*, No. 15-cr-381, *indictment filed,* 2015 WL 4749247 (E.D.N.Y. Aug. 5, 2015).

[2] *SEC v. Dubovoy et al.*, No. 15-cv-06076, *complaint filed* (D.N.J. Aug. 10, 2015). The SEC also alleged that the trading defendants violated Section 20(e) of the Exchange Act by aiding and abetting the computer hacker defendants and violated Section 20(b) of the Exchange Act by acting through the computer hacker defendants.

[3] The commentary does not address any of the other counts in the criminal cases, several of which may be easier for the government to prove than the securities fraud counts.

[4] Of course, the New Jersey courts are not bound by the 2nd Circuit's decision in *Dorozhko*. The 3rd Circuit has not considered whether computer hacking is a deceptive device within the meaning of Section 10(b) and Rule 10b-5.

[5] *Chiarella v. United States,* 445 U.S. 222, 235 (1980).

[6] The Court of Appeals remanded the case to the District Court to determine whether the computer hacking involved a fraudulent misrepresentation that was "deceptive" within the ordinary meaning of Section 10(b) and Rule 10b-5. The case was settled before the District Court made any findings on remand.

[7] The SEC civil complaint contains similar allegations. The SEC alleged the hacker defendants used deceptive means to gain unauthorized access to the newswires computer systems such as "(a) employing stolen username/password information of authorized units to pose as authorized users; (b) deploying malicious computer code designed to delete evidence of the computer attacks; (c) concealing the identity and location of the computers used to access the Newswire Services' computers; and (d) using back-door access-modules."

[8] On Sept. 14 two of the trading defendants — Ukrainian investment bank Jaspen Capital Partners Ltd. and CEO Andri Supranonok, neither of whom were charged criminally — entered into consent judgments with the SEC in which they agreed, without admitting or denying liability, to disgorge $30 million in trading profits.

[9] *Dirks v. SEC*, 463 U.S. 646 (1983).

[10] *United States v. Newman*, 773 F.3d 438 (2d Cir. 2014). The Court of Appeals in *Newman* further held that to the extent *Dirks* suggests that a personal benefit may be inferred from a personal relationship "where the tippee's trades 'resemble trading by the insider himself followed by a gift of the proceeds to the recipient,'" such an inference is improper unless there is proof of a "meaningfully close personal relationship that generates an exchange that is objective, consequential, and represents at least a potential gain of a pecuniary or similar valuable nature." The government had filed a petition for writ of *certiorari* seeking review of the court's holding as to what constitutes a personal benefit but not its holding that to be liable the tippee must know the tipper received a personal benefit, but the Supreme Court denied the request Oct. 5

Robert A. Horowitz (L) is a shareholder with **Greenberg Traurig** in New York, where he co-chairs the securities litigation practice. **Geoffrey S. Berman** (R) is a co-managing shareholder in the firm's Florham Park, N.J., office and is a shareholder in its New York office.