Marquette Law Review

Volume 94
Issue 4 *Summer 2011*

Article 8

SEC v. Dorozhko's Affirmative Misrepresentation Theory of Insider Trading: An Improper Means to a Proper End

Elizabeth A. Odian

SEC V. DOROZHKO'S AFFIRMATIVE MISREPRESENTATION THEORY OF INSIDER TRADING: AN IMPROPER MEANS TO A PROPER END

Historically, prosecution under Section 10(b) of the Securities and Exchange Act of 1934 has been limited to cases of nondisclosure fraud involving breach of a fiduciary duty to the corporation, its shareholders, or the source of the material nonpublic information. Some legal scholars criticize the limited scope of this law, arguing that it creates a loophole through which persons may trade on stolen material nonpublic information without fear of prosecution.

Bringing this issue to the forefront was a 2009 case, SEC v. Dorozhko, involving a Ukrainian citizen who hacked into a company's secure computer network where he accessed corporate financials prior to their release. In its opinion, the Second Circuit Court of Appeals greatly extended the reach of the SEC's policing power by adopting a new theory of insider, which eliminates the fiduciary duty requirement in cases involving an affirmative misrepresentation rather than a nondisclosure. In light of the court's unprecedented holding, this note examines the second circuit's approach, arguing that the Circuit impermissibly combined two distinct theories of securities fraud. Notwithstanding the second circuit's flawed approach, this note goes on to argue that computer hacking carried out in connection with securities trades should be condemned by the securities laws under the fraud on the investor theory of insider trading as a matter of public policy.

I. INTRODUCTION

Trading on material nonpublic information continues to be a hot-button issue on Wall Street as investors are continually searching for and trading on informational advantages.[1] With corporate America

1. Susan Pulliam et al., *U.S. in Vast Insider Trading Probe*, WALL ST. J., Nov. 20, 2010, at A1.

becoming increasingly digitalized, outsiders are finding new ways to obtain an informational advantage, such as hacking into secured computer networks housing confidential corporate information.[2] To adapt to these new technological developments and to root out fraudulent schemes carried out using the internet, the Securities & Exchange Commission ("SEC") established the Office of Internet Enforcement ("OIE") in 1998.[3] Since that time, the SEC has identified and prosecuted numerous hackers for engaging in fraudulent schemes in connection with securities transactions.[4]

Congress has never defined insider trading, leaving it to the courts to determine the extent of the prohibition. Guided by only the 1934 Securities and Exchange Act's vague prohibition against purchasing or selling securities using deceptive devices,[5] the Supreme Court has interpreted the deception element of insider trading to require a breach of a fiduciary duty owed by the trader to either the company, its shareholders, or the source of the material nonpublic information.[6] If a trader owes such a duty, he or she must "disclose or abstain" from trading on the nonpublic information.[7] As such, historically the SEC found only company insiders,[8] temporary insiders,[9] misappropriators,[10]

2. *See, e.g.*, Devlin Barrett et al., *Nasdaq Confirm Breach in Network*, WALL ST. J., Feb. 7, 2011, at C1.

3. Press Release, SEC, SEC Creates Office of Internet Enforcement to Battle Online Securities Fraud (July 28, 1998), *available at* http://www.sec.gov/news/digest/1998/dig072898.pdf. The SEC restructured the Division of Enforcement in early 2010. As a result, the Office of Internet Enforcement was dissolved. *See* Press Release, SEC, SEC Names New Specialized Unit Chiefs and Head of New Office of Market Intelligence (Jan. 13, 2010), *available at* http://www.sec.gov/news/press/2010/2010-5.htm.

4. Troy A. Paredes, Commissioner, SEC, Remarks Before the CyberSecurities Fraud Forum (Sept. 23, 2008), *available at* http://www.sec.gov/news/speech/2008/spch092308tar.htm. *See, e.g.*, Blue Bottle Ltd., Litig. Release No. 20018, 90 SEC Docket 268 (Feb. 26, 2007); Lohmus Haavel & Viisemann, Litig. Release No. 19450, 86 SEC Docket 1591 (Nov. 1, 2005). In both cases, the court granted the SEC its requested relief but declined to issue a written opinion. *Id.*; *see also* SEC v. Dorozhko, 574 F.3d 42, 50–51 (2d Cir. 2009) (finding that a computer hacker could be liable under section 10(b) and Rule 10b-5 should the lower court find that computer hacking is deceptive under the statute).

5. *See, e.g.*, 15 U.S.C. §§ 78a, 78j(a)–(b), 78i(a), 78(k) (2006).

6. *See* United States v. O'Hagan, 521 U.S. 642, 660 (1997) (holding that the defendant had committed fraud through nondisclosure because the defendant had a duty to disclose to the source of the information (his firm) that he would trade on); Chiarella v. United States, 445 U.S. 222, 235 (1980) (holding that "a duty to disclose under section 10(b) does not arise from the mere possession of nonpublic market information").

7. The disclose or abstain rule requires investors who wish to trade on the basis of nonpublic information to either disclose such information or abstain from trading altogether.

8. Corporate insiders include corporate directors, officers, employees, and other permanent insiders. *O'Hagan*, 521 U.S. at 652.

and tippees[11] liable for insider trading under Section 10(b) and Rule 10b-5. Outsiders with no fiduciary duty have avoided liability.[12]

On numerous occasions, the Supreme Court has rejected the parity of information approach to insider trading that would prohibit all trades made on nonpublic information irrespective of how the information was obtained.[13] Of course, the SEC has found that such a limitation frustrates its ability to regulate the securities market. To avoid this frustration, the SEC has continually sought to expand its regulatory power to reach all trades made on informational advantages.[14] Despite repeated rejections, the SEC has continued to strive for something close to parity by chipping away at the Court's initially narrow interpretation of Section 10(b) and Rule 10b-5—their latest victory being the Second Circuit's unprecedented decision in *SEC v. Dorozhko*.[15]

In *Dorozhko* the Second Circuit Court of Appeals held that computer hacking may be deemed a "deceptive device" under Section 10(b) of the Securities Exchange Act of 1934, despite the absence of a fiduciary duty.[16] Criticisms of the decision surfaced immediately, especially from legal scholars who interpreted prior Supreme Court precedent to foreclose insider trading liability under Section 10(b) and Rule 10b-5 where an outsider owes no fiduciary duty to the company, its

---

9. Temporary insiders include attorneys, accountants, consultants, and others who become temporary fiduciaries of a corporation. *Id.* (citing Dirks v. SEC, 463 U.S. 646, 655 n.14 (1983)).

10. Misappropriators include corporate outsiders who owe a fiduciary duty to the source of material nonpublic information, usually a corporate insider. *O'Hagan*, 521 U.S. at 652–53.

11. A tippee is a person who "assumes a fiduciary duty to the shareholders of a corporation not to trade on material nonpublic information only when the insider has breached his fiduciary duty to the shareholders by disclosing information to the tippee, and the tippee knows or should know that there has been a breach." *Dirks*, 463 U.S. at 660. A tippee may also be liable where he receives information from misappropriators or other tippees who breach a fiduciary duty of which the tippee is aware or should be aware. Robert A. Prentice, *The Internet and Its Challenges for the Future of Insider Trading Regulation*, 12 HARV. J. L. & TECH. 263, 296 (1999).

12. *See Dirks*, 463 U.S. at 665–67.

13. *Id.* at 656–59; *see also* Chiarella v. United States, 455 U.S. 222, 232 (1980).

14. *See Illegal Insider Trading: How Widespread is the Problem and is There Adequate Criminal Enforcement?: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. 138–139 (2006) (statement of Linda C. Thomsen, Director, Division of Enforcement, SEC).

15. *See, e.g.*, United States v. O'Hagan, 521 U.S. 642, 653 (1997) (extending 10(b) and Rule 10b-5 to misappropriators who breach a fiduciary duty to the source of nonpublic information); SEC v. Dorozhko, 574 F.3d 42, 50 (2d Cir. 2009) (eliminating the fiduciary duty requirement in cases involving affirmative misrepresentations rather than nondisclosures).

16. *Dorozhko*, 574 F.3d at 51.

shareholders, or the source.[17] Because computer hackers owe no fiduciary duty, their conduct, while punishable under wire fraud and computer fraud statutes,[18] would not constitute insider trading.[19]

Focusing on *Dorozhko* and computer hacking in general, this Note will discuss the development and future of insider trading laws as they apply to outsiders owing no fiduciary duty. To that end, Part II will provide a historical background of insider trading law from its common law origins to the Supreme Court's interpretation of Section 10(b) and Rule 10b-5 in the seminal opinions in *Chiarella v. United States*,[20] *Dirks v. SEC*,[21] and *United States v. O'Hagan*.[22] Part III will then discuss the Second Circuit Court of Appeals' recent decision in *SEC v. Dorozhko*, which greatly extended the reach of the SEC's policing power by eliminating the fiduciary duty requirement if the case involves an affirmative misrepresentation rather than a nondisclosure. Part IV will briefly address the lingering question of whether computer hacking is deceptive in the first place. Part V will then argue that the Second Circuit impermissibly combined two distinct theories of securities fraud: nondisclosure fraud or "insider trading," and affirmative misrepresentations or "fraud in connection with" a securities transaction. To illustrate the point, this section will begin with a discussion of the two theories, followed by an analysis of why computer hacking does not fall into the broader category not addressed by the SEC or the Second Circuit, focusing on both elements of the action—fraud and "in connection with" a securities transaction. Part VI will

---

17. *See, e.g.*, ProfessorBainbridge.com, The Second Circuit's Egregious Decision in SEC v. Dorozhko, (July 29, 2009) http://www.professorbainbridge.com/professorbainbridgecom/2009/07/the-second-circuits-recent-decision-in-sec-v-dorozhko-available-here-dealt-with-one-of-the-questions-left-open-by-the.html; *SEC v. Dorozhko: Second Circuit Dispenses With Fiduciary Duty Requirement in Hacker Insider Trading Case*, SECURITIES DOCKET, July 23, 2009, http://www.securitiesdocket.com/2009/07/23/sec-v-dorozhko-second-circuit-dispenses-with-fiduciary-duty-requirement-in-hacker-insider-trading-case/ (citing online discussion with Peter Henning); Posting of Joel M. Cohen to The Harvard Law School Forum on Corporate Governance and Financial Regulation, http://blogs.law.harvard.edu/corpgov/2010/07/29/erosion-of-the-fiduciary-duty-requirement-in-insider-trading-actions/ (July 29, 2009, 9:22 CST).

18. *See, e.g.*, 18 U.S.C. § 1030 (2006). For a list of state computer fraud and unauthorized access laws visit NCSL.org, Computer Hacking and Unauthorized Access Laws, http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/ComputerHackingandUnauthorizedAccessLaws/tabid/13494/Default.aspx (last visited May 18, 2011).

19. Robert Steinbuch, *Mere Thieves*, 67 MD. L. REV. 570, 589 (2008).

20. 455 U.S. 222 (1980).

21. 463 U.S. 646 (1983).

22. 521 U.S. 642 (1997).

argue that, notwithstanding the Second Circuit's flawed approach, computer hacking carried out in connection with securities trades should be condemned by Rule 10b-5 as a matter of public policy. Finally, Part VII will discuss alternative theories of insider trading that would proscribe trades made on nonpublic information obtained through computer hacking, arguing fidelity to Chief Justice Burger's fraud on the investor theory.

II. THE DEVELOPMENT OF INSIDER TRADING LAW

A. Early Insider Trading Law

At the turn of the twentieth century, state law governed securities transactions.[23] Many states permitted insiders to trade on the basis of material, nonpublic information.[24] By many, it was considered a perk for corporate investors.[25] While insiders could not affirmatively misrepresent their company's position, insiders owed no duty to disclose material information prior to trading on that information through the stock exchange.[26] An insider had only a duty to disclose material information prior to face-to-face transactions between buyer and seller.[27]

It was not until the 1929 Wall Street stock crash and subsequent depression that Congress passed the first federal securities laws[28] through the Securities and Exchange Acts of 1933 and 1934[29] ("Securities Act"). Congress intended for the Securities Act to reassure and protect investors while also reestablishing the integrity of the stock markets.[30] The 1934 Securities Act addressed insider trading in two sections, Section 16[31] and Section 10(b),[32] the latter being more relevant

23. STEPHEN M. BAINBRIDGE, SECURITIES LAW: INSIDER TRADING 3 (1999).

24. *Id.* at 1–3.

25. ELIZABETH SZOCKYJ, THE LAW AND INSIDER TRADING: IN SEARCH OF A LEVEL PLAYING FIELD 5 (1993).

26. Goodwin v. Agassiz, 186 N.E. 659, 661 (Mass. 1933) (noting that "mere silence does not usually amount to a breach of duty" particularly in cases where trades occur over the stock exchange rather than face-to-face).

27. *See id.*

28. BAINBRIDGE, *supra* note 23, at 23.

29. Ch. 404, 48 Stat. 881 (1934) (codified as amended at 15 U.S.C. §§ 78a–78lll (2006)).

30. BAINBRIDGE, *supra* note 23, at 23.

31. Securities Exchange Act of 1934, ch. 404, § 16, 48 Stat. 881 (codified as amended at 15 U.S.C. § 78p (2006)). Section 16 proscribes the use of nonpublic material information by corporate insiders for purposes of securities trading. *Id.*

32. Securities Exchange Act of 1934, ch. 404, § 10(b), 48 Stat. 881 (codified as amended at 15 U.S.C. § 78j(b)). The full text reads:

to this Note.

Section 10(b) of the Securities Act prohibits the use or employment of any "manipulative" or "deceptive device" in connection with the purchase or sale of any security that contravenes SEC rules and regulations.[33] The SEC intended Section 10(b) to act as a "catch-all" clause to prevent fraudulent practices within the securities markets.[34] On its face, Section 10(b) does not mention insider trading nor does it make any conduct unlawful.[35] Rather, it grants the SEC authority to pass rules forbidding the use of "manipulative" or "deceptive devices" in connection with securities transactions.[36] Pursuant to this rulemaking authority, the SEC later promulgated Rule 10b-5 in 1948.[37] Rule 10b-5 prohibits the use of "any device, scheme, or artifice to defraud" and "any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person."[38] In effect, the laws forbid "(1) using any deceptive device (2) in connection with the purchase or sale of securities, in contravention of [Rule 10b-5]."[39]

For nearly twenty years, the SEC only used Rule 10b-5 to prosecute insiders who fraudulently misrepresented their company's position for

---

> It shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce or of the mails, or of any facility of any national securities exchange . . . [t]o use or employ, in connection with the purchase or sale of any security registered on a national securities exchange or any security not so registered, or any securities-based swap agreement (as defined in section 206B of the Gramm-Leach-Bliley Act [15 U.S.C.S. § 78c note]), any manipulative or deceptive device or contrivance in contravention of such rules and regulations as the Commission may prescribe as necessary or appropriate in the public interest or for the protection of investors.

Id.

33. *Id.* Insider trading is but one form of deception covered under the statute. There is also a private cause of action for simple fraud where an insider makes an affirmative misrepresentation affecting the market price of the company's securities. *See, e.g.*, Deutschman v. Beneficial Corp., 841 F.2d 502, 504, 506, 508 (3d Cir. 1988) (holding that a corporate manager who makes affirmative misrepresentations that, in effect, artificially support the market price of the company's stock, may be liable under Section 10(b)); Liebhard v. Square D Co., 811 F. Supp. 354, 354–56 (N.D. Ill. 1992); Margolis v. Caterpillar, Inc., 815 F. Supp. 1150, 1155 (C.D. Ill. 1991).

34. Ernst & Ernst v. Hochfelder, 425 U.S. 185, 202–04, 206 (1976).

35. *See* Securities Exchange Act of 1934, ch. 404, § 16, 48 Stat. 881 (codified as amended at § 15 U.S.C. § 78j(b)).

36. *See id.*

37. 17 C.F.R. § 240.10b-5 (2006).

38. *Id.*

39. United States v. O'Hagan, 521 U.S. 642, 651 (1997).

personal gain.[40] The SEC first applied the rule to an outsider trading on inside information in the case *In re Cady, Roberts & Co*.[41] In that case, Robert Gintel, a selling broker, purchased thousands of shares of Curtiss-Wright stock.[42] Shortly thereafter, Curtiss-Wright decided to reduce its quarterly dividends.[43] Gintel's partner, J. Cheever Cowdin, who was also a member of Curtiss-Wright's board of directors, informed Gintel of the company's decision.[44] Based on that information, Gintel sold several thousand shares of the company's stock prior to Curtiss-Wright's public announcement, avoiding major losses for his clients.[45]

The SEC found that Gintel violated Rule 10b-5 by trading on nonpublic, material information, holding that "insiders must disclose material facts which are known to them by virtue of their position but which are not known to persons with whom they deal and which, if known, would affect their investment judgment."[46] If full disclosure would be "improper or unrealistic under the circumstances," the party must abstain from trading.[47] Thus, the "disclose or abstain" rule was born, requiring that insiders either disclose material information prior to trading in company stock or abstain from trading altogether. The SEC then outlined two principles supporting a disclosure requirement.[48] First, the SEC reasoned that a relationship that affords one with direct or indirect access to material information intended only for corporate persons should not be used for personal gain.[49] Second, the SEC reasoned that disclosure should be necessary where it would be inherently unfair for one with access to material information to take advantage of that information, to the detriment of those without such knowledge.[50] How the party obtained the information was irrelevant.[51]

Because *In re Cady, Roberts & Co* was an administrative decision, it did not hold much weight. However, the Second Circuit Court of

40. BAINBRIDGE, *supra* note 23, at 28.
41. *See generally In re* Cady, Roberts & Co., 40 S.E.C. 907 (1961).
42. *Id.* at 908.
43. *Id.* at 909.
44. *Id.*
45. *Id.*
46. *Id.* at 911.
47. *Id.*
48. *Id.* at 912.
49. *Id.*
50. *Id.*
51. *See id.* at 910–911.

Appeals later adopted the rule in *SEC v. Texas Gulf Sulphur Co.*[52] In *Texas Gulf Sulphur*, corporate officers were charged under Section 10(b) and Rule 10b-5 after trading in company securities prior to the public announcement of a large mineral strike.[53] The court held that any person who traded on inside information would be liable under Section 10(b) and Rule 10b-5, whether he accessed that information directly or indirectly, so long as he knew that the information was not available to those with whom he traded.[54] The court then provided four elements a party must prove to establish liability under the statute: (i) a fraud or omission (ii) of material fact (iii) made in connection with the purchase or sale of securities (iv) with scienter[55] or intent to deceive by way of omission.[56] Today, these four elements are still required; however, later Supreme Court decisions would greatly narrow the scope of the *Texas Gulf Sulpher* holding.[57]

B. Classical Theory: Limiting Insider Trading Liability to Corporate Insiders

In 1979, the Supreme Court greatly narrowed the reach of Section 10(b) and Rule 10b-5 by limiting the "disclose or abstain" rule to situations where the buyer and seller had a relationship of trust and confidence.[58] This is known as the "traditional" or "classical" theory of insider trading.[59] In situations where an insider wishes to trade on information known to him solely by virtue of his position within the corporation, he must either publicly disclose the material information on which he wishes to trade or abstain from trading on that information altogether.[60] Such insider trading is considered a "deceptive device" because corporate insiders owe a fiduciary duty to their shareholders.[61]

52. SEC v. Texas Gulf Sulphur Co., 401 F.2d 833, 848 (2d Cir. 1968).

53. *Id.* at 847–50.

54. *Id.* at 852.

55. Scienter is defined as the "mental state embracing intent to deceive, manipulate, or defraud." Ernst & Ernst v. Hochfelder, 425 U.S. 185, 193–94 n.12 (1976).

56. *See generally Texas Gulf Sulphur*, 401 F.2d 833.

57. *See, e.g.*, Chiarella v. United States, 455 U.S. 222, 229–30 (1980). *See generally* United States v. O'Hagan, 521 U.S. 642 (1997).

58. *Chiarella*, 455 U.S. at 228.

59. *See O'Hagan*, 521 U.S. at 652.

60. *See generally In re* Cady, Roberts & Co., 40 S.E.C. 907 (1961). Corporate insiders include corporate officers, directors, controlling stockholders, company employees, attorneys, accountants, and any other consultants who become temporary fiduciaries of the corporation. *O'Hagan*, 521 U.S. at 652 (citing Dirks v. SEC, 463 U.S. 646, 655 n.14 (1983)).

61. *O'Hagan*, 521 U.S. at 652.

When the insider trades on nonpublic information, he breaches this duty and deceives shareholders by taking unfair advantage of his inside knowledge—knowledge unavailable to the shareholder.[62] In effect, under the classical theory, a fiduciary duty to the company's shareholders is a required element of "deceptive device."[63]

The Supreme Court first narrowed the scope of *Texas Gulf Sulpher* in its *Chiarella v. United States* opinion. Chiarella, an employee of Pandick Press, a financial printing company, was charged under Section 10(b) and Rule 10b-5 for trading on inside information regarding five impending corporate takeovers.[64] He discovered this information by deciphering certain information contained in documents he handled while in the employment of Pandick Press.[65] The lower court ruled that all those who possess inside information must disclose or abstain from trading on such information; the Supreme Court, however, rejected this theory upon review for failure to meet the "deceptive device" requirement.[66] Because in cases of nondisclosure there "can be no fraud [i.e., deception] absent a duty to speak," the Court held that Chiarella did not violate Section 10(b) or Rule 10b-5 because he owed no duty to disclose.[67] The Court explained that mere possession of material nonpublic information does not create a duty to disclose under Section 10(b).[68] A fiduciary duty between the parties is required. This fiduciary "duty ar[ises] from (i) the existence of a relationship affording access to inside information intended to be available only for a corporate purpose, and (ii) the unfairness of allowing a corporate insider to take advantage of that information by trading without disclosure."[69] The Supreme Court reiterated this point four years later in its decision in *Dirks v. SEC*, stating that:

> We were explicit in *Chiarella* in saying that there can be no duty to disclose where the person who has traded on inside information "was not [the corporation's] agent, . . . was not a fiduciary, [or] was not a person in whom the

62. *Id.*

63. *Chiarella*, 455 U.S. at 228.

64. *Id.* at 224–25.

65. *Id.* at 224.

66. United States v. Chiarella, 588 F.2d 1358, 1364 (2d Cir. 1978), *rev'd*, 445 U.S. 222, 237 (1980).

67. *Chiarella*, 445 U.S. at 235.

68. *Id.*

69. *Id.* at 227 (citing Cady, Roberts & Co., 40 S.E.C. 907, 912 (1961)).

> sellers [of the securities] had placed their trust and confidence." Not to require such a fiduciary relationship, we recognized, would "[depart] radically from the established doctrine that duty arises from a specific relationship between two parties" and would amount to "recognizing a general duty between all participants in market transactions to forgo actions based on material, nonpublic information."[70]

In *Dirks*, the Court extended insider trading liability to tippers and tippees. Dirks, an officer at a New York broker-dealer firm, received notice from a former officer at Equity Funding of America that the company grossly overstated its assets by engaging in fraudulent practices.[71] Dirks then confirmed these allegations through a personal investigation.[72] Neither Dirks nor his firm owned or traded in the insurance company's securities, but Dirks did disclose this information to a number of clients and investors who did in fact own Equity Funding securities.[73] Upon receiving this information, many of these shareholders elected to sell their share of the company, avoiding huge losses incurred by uninformed shareholders as news of the fraud became public.[74] Soon after, the SEC investigated Dirks' role in uncovering the fraud and subsequently charged Dirks for insider trading in violation of Section 10(b) and rule 10b-5.[75] Adhering to its decision in *Chiarella*, the Court held that one's duty to disclose material nonpublic information prior to trading arises not from possessing the information, but rather from the relationship between the parties.[76] Therefore, despite aiding and abetting investors by tipping them of the fraud allegations, Dirks was not liable under Section 10(b) and Rule 10b-5 because, as a broker, he owed no duty to Equity Funding or its shareholders.[77] The import of this decision is that a tippee owes a fiduciary duty to company shareholders only when the insider shares nonpublic material information in breach of his fiduciary duty to company shareholders, and both the tipper and tippee are aware that such duty was breached.[78]

---

70. Dirks v. SEC, 463 U.S. 646, 655 (1983) (quoting *Chiarella*, 445 U.S. at 232–33).
71. *Dirks*, 463 U.S. at 648–49.
72. *Id.* at 649.
73. *Id.*
74. *Id.* at 649–50.
75. *Id.*
76. *Id.* at 657–658.
77. *Id.* at 665.
78. *Id.* at 660.

Here, Dirks, a stranger to Equity Funding, owed no such duty.[79]

C. Misappropriation Theory: Extending Insider Trading Liability to Outsiders Owing a Fiduciary Duty to Their Source

Because the classical theory reached only persons who owed a fiduciary duty to company shareholders, the minority in *Chiarella* endorsed a more encompassing theory of liability, known as the misappropriation theory.[80] The misappropriation theory of insider trading makes it illegal to trade securities based on misappropriated, nonpublic information.[81] Two versions of the theory exist—the "fraud on the investor" theory and the "fraud on the source" theory.[82]

1. Fraud on the Investor Theory

In his dissenting opinion in *Chiarella*, Chief Justice Burger proposed a broad reading of Section 10(b) and Rule 10b-5, which would extend liability to *any* person who misappropriated nonpublic information using *any* deceptive device.[83] Recognizing that silence is generally permitted during business transactions unless the parties have a fiduciary relationship,[84] Chief Justice Burger argued that liability should attach when a person obtains an informational advantage "not by superior experience, foresight, or industry, but by some unlawful means."[85] Building on this principle, he advocated holding all persons to the same standard as insiders, requiring any person who misappropriated material nonpublic information to disclose or abstain from trading on it altogether.[86]

---

79. *Id.* at 667.

80. *See* Chiarella v. United States, 455 U.S. 222, 237–52 (1980) (Stevens, J., concurring; Burger, C.J., dissenting; Blackmun, J., dissenting).

81. Barbara Bader Aldave, *Misappropriation: A General Theory of Liability for Trading on Nonpublic Information*, 13 HOFSTRA L. REV. 101, 114 (1984).

82. *See Chiarella*, 445 U.S. at 237–252.

83. *Id.* at 240 (Burger, C.J., dissenting).

84. This general rule "permits a businessman to capitalize on his experience and skill in securing and evaluating relevant information [providing] incentive for hard work, careful analysis, and astute forecasting." *Id.* at 239.

85. *Id.* at 239–240.

86. *Id.* at 240.

2. Fraud on the Source Theory

"Fraud on the source" liability was a narrower version of the misappropriation theory espoused by Justice Stevens in his concurring opinion.[87] He posited that when Chiarella bought securities in the open market, he violated a duty of silence owed to his employers and its customers, the source of material nonpublic information.[88] The Supreme Court later adopted this theory in *O'Hagan*.[89]

O'Hagan was partner at Dorsey & Whitney law firm.[90] Grand Met engaged Dorsey & Whitney as local counsel to manage a potential tender offer for the Pillsbury Company's common stock.[91] O'Hagan himself was not involved in the tender offer; however, with knowledge of the offer, O'Hagan purchased approximately 2500 call options for Pillsbury stock and another 5000 shares of common stock.[92] When Grand Met announced the tender offer, the share value increased significantly. O'Hagan exercised his call options and sold his common stock realizing a profit of more than $4.3 million.[93]

The Court found O'Hagan liable under Section 10(b) and Rule 10b-5, holding that "a person who trades in securities for personal profit, using confidential information misappropriated in breach of a fiduciary duty to the source of the information, may be held liable for violating Section 10(b) and Rule 10b-5."[94] O'Hagan's failure to disclose his actions to Grand Met and Dorsey & Whitney was deceptive because he

87. *Id.* at 237 (Stevens, J., concurring). Justice Stevens suggested that Chiarella violated Section 10(b) under a narrow version of the misappropriation theory, but concurred in the result because Chiarella's counsel did not make that argument at trial. *Id.* at 238.

88. *Id.* at 237.

89. *See* United States v. O'Hagan, 521 U.S. 642, 655 (1997). According to the misappropriation theory, a person violates Rule 10b-5 when he: "(1) misappropriates material[,] nonpublic information, (2) by breaching a duty arising out of a relationship of trust and confidence[,] and (3) uses that information in a securities transaction, (4) regardless of whether he owed any duty to the shareholders of the traded stock." SEC v. Clark, 915 F.2d 439, 443 (9th Cir. 1990). The SEC has successfully argued the misappropriation theory to impose liability on (1) traditional company insiders, including officers, directors, and senior management, O'Connor & Assocs. v. Dean Witter Reynolds, Inc., 529 F. Supp. 1179, 1185, 1187–88 (S.D.N.Y. 1981), (2) rank-and-file employees who breached a fiduciary duty to their employers, SEC v. Cherif, 933 F.2d 403, 410–12 (7th Cir. 1991), and (3) temporary insiders, SEC v. Tome, 638 F. Supp. 596, 620–22 (S.D.N.Y. 1986), and (4) possibly family members, United States v. Willis, 778 F. Supp. 205, 208–09 (S.D.N.Y. 1991). *But c.f.* United States v. Chestman, 947 F.2d 551, 568–71 (2d Cir. 1991).

90. *O'Hagan*, 521 U.S. at 647.

91. *Id.*

92. *Id.* at 647–48.

93. *Id.* at 648.

94. *Id.* at 646.

had a duty to of nondisclosure to his employer.[95] Essentially, the breach of duty to the source constitutes the requisite deception.[96] Had O'Hagan disclosed to his employer his intent to trade, his duty would have been satisfied, and he would not have been subject to Rule 10(b)5.

Moreover, the Court determined that the misappropriation theory satisfied the "in connection with" element of a Rule 10b-5 action. The Court reasoned that his conduct was "in connection with the purchase or sale of a security" because O'Hagan completed the fraud when, without disclosure to his law firm, he used the information to purchase and then sell Pillsbury stock, not when he received the confidential information.[97] Had O'Hagan used the nonpublic information for purposes unrelated to a securities transaction, he would not be subject to Rule 10b-5 because the rule does not capture all forms of fraud involving nonpublic information, but only those used to capitalize on such information.[98]

III. *SEC v. Dorozhko*: Eliminating the Fiduciary Duty Requirement

The *O'Hagan* decision was so significant because it expanded Section 10(b) and Rule 10b-5 liability to corporate outsiders who owe no fiduciary duty to the corporation or its shareholders. The Court elected to base liability, instead, upon the fiduciary duty owed to the source of the material information.[99] However, critics insisted that the Court adopted an overly restrictive version of misappropriation liability that frustrates the prosecution of defendants who trade on misappropriated information acquired through other means.[100] The Second Circuit attempted to close this gap by holding that the breach of a fiduciary duty is not a required element of "deceptive device."[101]

95. *Id.* at 660.

96. *Id.*

97. *Id.* at 656.

98. *Id.*

99. *See id.* at 660.

100. Donna M. Nagy, *Reframing the Misappropriation Theory of Insider Trading Liability: A Post-*O'Hagan *Suggestion*, 59 OHIO ST. L.J. 1223, 1225–26 (1998). To illustrate, because a computer hacker has no connection whatsoever—let alone a fiduciary relationship—with the source of confidential information, some scholars have concluded that computer hacking lacks the type of deception essential to the misappropriation theory, namely "feigned fidelity" to the source. *See id.* at 1247, 1253, 1254, 1262, 1263. Thus, the misappropriation theory would not extend to cases where the defendant trades on information gained illegally through computer hacking.

101. SEC v. Dorozhko, 574 F.3d 42, 49–50 (2d Cir. 2009).

A. The Case: Dorozhko Hacks and Trades

In early October 2007, IMS Health, Inc. announced that it would release its third-quarter financials after the securities markets closed at 5:00 p.m. on October 17, 2007.[102] Thomson Financial, Inc., an investor relations and web-hosting firm, managed IMS Health's release.[103]

On the afternoon of October 17, 2007, Dorozhko hacked into a secure server at Thomson Financial and downloaded IMS Health's earnings report.[104] Shortly before 3:00 p.m., Dorozhko purchased $41,670.90 worth of put options in IMS Health stock.[105] This amounted to approximately ninety percent of all put options purchased in the previous six-week period.[106] As announced, that evening IMS Health released its third-quarter earnings, which were twenty-eight percent lower than Wall Street expectations.[107] When the market opened the next morning, the value of IMS Health's stock declined approximately twenty-eight percent.[108] The defendant sold his options within six minutes of the opening bell, realizing a profit of $286,456.59 overnight.[109]

The SEC received notice of this irregular trading activity and successfully sought a temporary restraining order preventing the defendant from accessing the funds in his brokerage account.[110] The United States District Court for the Southern District of New York later denied the SEC's request for a preliminary injunction for failure to show likelihood of success on the merits, reasoning that, as a matter of law, "computer hacking was not 'deceptive' within the meaning of Section 10(b) as defined by the Supreme Court."[111] The court stated that "a breach of a fiduciary duty of disclosure is a required element of any 'deceptive' device under section 10(b)."[112] Owing no duty to either IMS Health shareholders or Thomson Financial, Dorozhko was not liable under Section 10(b) and Rule 10b-5, despite violating a number of state and federal statutes criminalizing computer hacking.[113] The SEC

102. *Id.* at 44.
103. *Id.*
104. *Id.*
105. *Id.*
106. *Id.*
107. *Id.*
108. *Id.*
109. *Id.* This amounted to approximately a 700% return on investment.
110. *Id.* at 44–45.
111. *Id.* at 45.
112. *Id.* (citing SEC v. Dorozhko, 606 F. Supp. 2d 321, 330 (S.D.N.Y. 2008)).
113. *Id.*

appealed.

B. The Second Circuit Court of Appeals Opinion Adopts a New "Affirmative Misrepresentation Theory of Insider Trading," Eliminating the Fiduciary Duty Requirement

On appeal, the SEC recognized that the facts did not fit under either the classical or "fraud on the source" misappropriation theory of insider trading because no fiduciary duty was breached.[114] Rather, it urged the court to recognize the alleged hacking as an affirmative misrepresentation, which would not require breach of a fiduciary duty to be fraudulent.[115] The court accepted the SEC's argument, overturned the district court's decision and remanded the case for further proceedings to determine whether computer hacking was "deceptive" or mere theft.[116]

In holding that a breach of fiduciary duty was not required for computer hacking to be "deceptive" under Section 10(b), the court distinguished fraud by nondisclosure from fraud by affirmative misrepresentation.[117] The court explained that previous Supreme Court decisions dealt only with cases of mere nondisclosure and that the common law theory of fraudulent nondisclosure requires breach of a fiduciary duty while the theory of fraudulent misrepresentation does not.[118] Neither *Chiarella, O'Hagan*, or *Dirks* precluded premising Section 10(b) liability on common law fraud. Chiarella's "case concern[ed] the legal effect of [his] silence."[119] Likewise, O'Hagan's case concerned his failure to disclose his intent to trade on material nonpublic information to the source, his employer.[120] Finally, Dirks' case concerned his failure to publicly disclose his knowledge of Equity Funding's fraudulent practices prior to tipping his clients.[121] In each case, the question of "deception" related to whether the defendant breached a fiduciary duty to disclose. In *Dorozhko* on the other hand,

114. *Id.*

115. *Id.*

116. *Id.* at 51. The district court denied the SEC's motion for a preliminary injunction holding that defendant's hack and trade did not violate section 10(b) because defendant did not breach a fiduciary duty in connection with the purchase or sale of a security. The alleged scheme was not manipulative because it did not control or artificially affect market activity. *Dorozhko*, 606 F. Supp. 2d at 329.

117. *Dorozhko*, 574 F.3d at 49–50.

118. *Id.*

119. Chiarella v. United States, 445 U.S. 222, 226 (1980).

120. United States v. O'Hagan, 521 U.S. 642, 647–48 (1997).

121. Dirks v. SEC, 463 U.S. 646, 649–50 (1983).

the question of "deception" related not to a breach of a fiduciary duty, but to an affirmative misrepresentation, which is deceptive in and of itself. Therefore, in cases involving misrepresentation, a fiduciary duty is not a required element of "deceptive device."[122] Because the court was aware of no Supreme Court case contravening this holding, it added that "[a]bsent a controlling precedent that 'deceptive' has a more limited meaning, we see no reason to complicate the enforcement of Section 10(b) by divining new requirements."[123] Essentially, the Second Circuit viewed its holding as simply paralleling the contours of common law fraud.

In addition, the court left open the question of whether computer hacking is deceptive in the first place. Despite asserting that "misrepresenting 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,"[124] the court hesitated to apply this general principle to the set of facts before it. Instead, it remanded the case to the district court to determine whether the computer hacking in this particular case involved an affirmative misrepresentation, deceptive within the ordinary meaning of Section 10(b). Upon remand, the court granted the SEC summary judgment after the motion went unopposed.[125]

IV. COMPUTER HACKING—"DECEPTIVE THEFT" OR "MERE THEFT?"

Because Dorozhko's case was dismissed upon an unopposed motion for summary judgment, the question still remains as to whether computer hacking is indeed "deceptive."[126] Prior to the Second Circuit's

122. *See id.* at 649–51. *But see* Regents of Univ. of Cal. v. Credit Suisse First Boston (USA), Inc., 482 F.3d 372, 389 & n.30 (5th Cir. 2007) (interpreting *Chiarella* and *O'Hagan* as "establish[ing] that a device, such as a scheme, is not 'deceptive' unless it involves breach of some duty of candid disclosure.").

123. *Dorozhko*, 574 F.3d at 49.

124. *Id.* at 51.

125. Dorozhko, Litig. Release No. 21465, 2010 WL 1213430 (Mar. 29, 2010).

126. *Dorozhko*, 574 F.3d at 51. Factual findings regarding the nature of Dorozhko's hacking were required because the record did not contain such information. First, Dorozhko elected to invoke his Fifth Amendment right to refrain from testifying. Second, Dorozhko "concealed his exit from the computer system," and third, Thomson Financial chose not to fully explore the details of Dorozhko's method of hacking so that it could protect certain trade secrets. Brief of Appellant at 24–25, SEC v. Dorozhko, 574 F.3d 42 (2d Cir. 2009) (No. 08-0201-CV). Upon remand, the SEC, in its motion for summary judgment, admitted that is still had not determined how Dorozhko gained access to Thomson's computers. Memorandum of Law in Support of Its Motion for Summary Judgment of Plaintiff at 14, SEC v. Dorozhko, No. 07-CIV-9606 (NRB) (S.D.N.Y. 2010). Further, beyond quoting the Second

Dorozhko opinion, legal scholars generally thought that theft of inside information, while punishable under criminal codes,[127] would not give rise to insider trading liability.[128] The reasoning behind this assumption was that liability based on an affirmative misrepresentation is actionable under Section 10(b) and Rule 10b-5 only if the court finds a false representation, in other words, a "lie."[129] So, for example, if a person forcefully broke into an office and stole material nonpublic information for the purpose of securities trading, the thief would be subject to criminal theft or burglary charges but free from insider trading liability because there was no lie.[130] The requisite fraud or deception would be missing.[131]

In its brief submitted to the Court of Appeals, the SEC argued that hackers gain access to nonpublic information stored on computer in two ways, both of which constitute affirmative misrepresentations.[132] First, hackers may falsely identify themselves by masquerading as other authorized users.[133] Second, a hacker might "exploit a weakness in an [electronic code] within a program" to grant him access to otherwise unavailable content.[134] In the court's view, "misrepresenting one's identity in order to gain access to information that is otherwise off limits, and then stealing that information is plainly 'deceptive.'"[135] For example, if a computer hacker accesses nonpublic information by using a password he is not authorized to use, he deceives the computer by impersonating the rightful user. This impersonation constitutes deception.[136] With companies increasingly turning to computers to perform tasks once completed by human beings, such as granting and

---

Circuit opinion, the SEC's brief in support of its summary judgment motion offered little argument as to why computer hacking should be deemed deceptive. It simply offered that Dorozhko accessed IMS Health's earnings "by infiltrating, tricking, and misleading Thomson Financial's highly complex and secure computer security systems." *Id.* at 12.

127. *See* sources cited *supra* note 18.

128. *See* sources cited *supra* note 4.

129. Stephen M. Bainbridge, *Ruling on Hackers as Inside Traders: Right in Theory, Wrong on the Law*, LEGAL BACKGROUNDER, Oct. 9, 2009, at 1, *available at* http://www.wlf.org/Upload/legalstudies/legalbackgrounder/100909Bainbridge_LB.pdf.

130. *See* SEC v. Dorozhko, 606 F. Supp. 2d 321, 339 (S.D.N.Y. 2008).

131. *Id.*

132. SEC v. Dorozhko, 574 F.3d 42, 50–51 (2d Cir. 2009).

133. *Id.*

134. *Id.*

135. *Id.* at 51.

136. Randall W. Quinn, Comment: *The Misappropriation Theory of Insider Trading in the Supreme Court: A (Brief) Response to the (Many) Critics of United States v. O'Hagan*, 8 FORDHAM J. CORP. & FIN. L. 865, 894–95 (2003).

denying access to confidential information once stored offline, there should be no distinction between deceiving a person or a computer.

The Second Circuit struggled with whether accessing unauthorized information stored on a computer by "exploiting code" was deception or mere theft. On one hand, this conduct parallels the thief who exploits the weakness in a building's security system in order to break in and *physically* steal information.[137] This conduct would not be deceptive because the theft was carried out by using force, not deceit.[138] On the other hand, code exploitation techniques may be characterized as allowing hackers "to take control of the target program's execution flow by *tricking* it into running a piece of malicious code that has been smuggled into memory."[139] Computer hackers may trick a computer into completing actions the hacker wants it to do even when the code, as written, was designed to prevent those actions.[140] Trickery is a form of deception; so, if this characterization were accepted, code exploitation would also be deceptive under Section 10(b) and Rule 10b-5.[141]

V. THE SECOND CIRCUIT EFFECTIVELY COMBINED TWO DISTINCT THEORIES OF SECURITIES FRAUD INTO ONE

Although computer hacking may be characterized as deceptive or fraudulent conduct, the link between such fraud and the securities transaction is misplaced. The Second Circuit's unprecedented holding—that a fiduciary duty is not an element of an insider trading case where an affirmative misrepresentation is involved—effectively combines two distinct theories of securities fraud by substituting an insider trading case's fiduciary duty analysis with a common law affirmative misrepresentation analysis.

By definition, insider trading cases involve nondisclosure fraud. In a typical scenario, a corporate insider purchases or sells stock after failing to disclose his superior knowledge to the public. Liability under Section 10(b) attaches because the insider breached his duty to disclose. This section will begin by distinguishing the two theories of fraud, then explain why the case cannot be proved under a traditional affirmative

137. *See id.* at 895.

138. *See id.*

139. JON ERICKSON, HACKING: THE ART OF EXPLOITATION 118 (2d ed. 2008) (emphasis added).

140. *Id.* at 87.

141. For a summary of various computer hacking techniques and an argument as to why each is deceptive under 10(b) see Michael D. Wheatley, *Apologia for the Second Circuit's Opinion in SEC v. Dorozhko*, 7 J.L. ECON. & POL'Y 25, 47–50 (2010).

misrepresentation theory.

A. Distinguishing Nondisclosure Fraud from Affirmative Misrepresentation Fraud

To establish a case under Section 10(b) and Rule 10b-5, there must be (1) a deceptive device (i.e., fraud) (2) in connection with the purchase or sale of securities, in contravention of Rule 10b-5.[142] Plaintiffs may bring claims under this general prohibition by arguing two theories of fraud: nondisclosure or affirmative misrepresentation. Nondisclosure cases are those cases traditionally referred to as "insider trading," while affirmative misrepresentation cases fall into a more general category of securities fraud which prohibits all fraud in connection with securities trades.

Insider trading involves the nondisclosure of material nonpublic information, gained not by skill or effort, but rather through the investor's relationship to the issuing company, its shareholders, or the source of his nonpublic information.[143] The "deceptive device" is the trader's breach of that fiduciary relationship.[144] The fiduciary duty requirement reflects the principles that mere possession of nonpublic information does not trigger a duty of disclosure[145] and that the federal securities laws target "the inappropriate and deceptive use of special relationships."[146] Where an investor receives nonpublic information through permissible channels and without an obligation to keep the information confidential or where the investor discloses the information to his fiduciary prior to trading, Section 10(b) and Rule 10b-5 do not forbid trades based on such information.[147] Again, computer hackers do not fit under this category of cases because the hacker owes no fiduciary duty.

Affirmative misrepresentation cases, on the other hand, generally involve a material misrepresentation made to the investing public for the purpose of inducing the sale or purchase of stock.[148] The

142. United States v. O'Hagan, 521 U.S. 642, 651 (1997).

143. *Id.* at 658–59.

144. *See* Chiarella v. United States, 445 U.S. 222, 228 (1980).

145. Dirks v. SEC, 463 U.S. 646, 651–54 (1983) (discussing Chiarella v. United States, 455 U.S. 222 (1980)).

146. Cohen, *supra* note 17.

147. *See Dirks*, 463 U.S. at 662–63.

148. *See, e.g.*, Deutschman v. Beneficial Corp., 841 F.2d 502, 506 (3d Cir. 1988) (holding that where a defendant's 10b-5 action is based on an affirmative misrepresentation which distorts the value of stock, the defendant need not have owe a fiduciary duty to the plaintiff to

misrepresentation involved is made by the defendant to induce someone else to enter into a securities transaction, not to inform his own securities transaction. These cases do not fall under the title of "insider trading," but rather under Section 10(b) and Rule 10b-5's general prohibition against fraud in connection with securities transactions. The "deceptive device" here is the material misrepresentation of fact. Finding a computer hacker liable under this theory is equally unprecedented as affirmative misrepresentation cases have never dealt with false statements made to computers.

B. Why an Affirmative Misrepresentation Made to A Computer is Not Punishable Under 10(b)'s General Prohibition Against Fraud Connection with a Securities Transaction

Likely recognizing that computer hacking would not fall under the general prohibition against fraud in connection with a securities transaction, the SEC argued for a new theory of insider trading, accepted by the Second Circuit, that substitutes the longstanding fiduciary duty requirement with a test for common law fraud. This section discusses why the SEC did not pursue a traditional affirmative misrepresentation cause of action. First, the SEC would have faced a significant hurdle in establishing fraud, namely the elements of materiality and reliance. Second, certain timing issues related to the consummation of the fraud arise with regard to the "in connection with" requirement.

1. Problems with Establishing Fraud

Although computer hacking may be characterized as fraudulent conduct, the link between such fraud and the securities transaction is misplaced. Under the common law, liability for mere nondisclosure requires a fiduciary duty to disclose.[149] This duty to disclose "arises when one party has information 'that the other [party] is entitled to know because of a fiduciary or other similar relation of trust and confidence between them.'"[150] However, liability for fraudulent misrepresentation does not.[151] To establish a prima facie case, the plaintiff must show that the defendant (i) made a false representation

---

be held liable).

149. RESTATEMENT (SECOND) OF TORTS § 551(1) (1976).

150. Chiarella v. United States, 455 U.S. 222, 228 (1980) (quoting RESTATEMENT (SECOND) OF TORTS § 551(2)(a)).

151. *See* RESTATEMENT (SECOND) OF TORTS § 525.

(ii) concerning a material fact (iii) "for the purpose of inducing [him] to act or to refrain from action," (iv) that he actually and justifiably relied upon the representation and (v) that his injury was caused by such reliance.[152] A computer hacker thus makes a false representation of material fact by falsely identifying himself to a computer system as an authorized user. The computer then relies on this misrepresentation when it grants access to the hacker. This false identification is made to induce the computer system into allowing him access he would otherwise not be granted. Breach of the computer system's security measures would result in injury when confidential information is stolen.

Even if computer hacking is deemed fraudulent, the definition of fraud under securities law does not mirror its definition under the common law. In fact, the Court has explicitly stated that "Section 10(b) does not incorporate common-law fraud into federal law."[153] Take for example the elements of materiality and reliance. Under 10(b) and Rule 10b-5, the fact must be material to the investor. Likewise, the investor must rely on the misrepresented material fact. It is not sufficient for there to be any material fact or reliance by anyone somewhere in the factual situation presented. Consequently, computer hacking does not fit neatly into a traditional affirmative misrepresentation case. The following discussion of the materiality and reliance requirements will further illuminate the point.

A statement is material if it is substantially likely that a reasonable investor would consider the information relevant to his decision to purchase or sell securities and if it "alter[s] the 'total mix' of information

152. *Id.*

153. Stoneridge Inv. Partners, LLC v. Scientific-Atlanta, Inc. 552 U.S. 148, 162 (2008) (citing SEC v. Zandford, 535 U.S. 813, 820 (2002)); *see also* Cohen, *supra* note 17. In his blog posting, Cohen argues that the Second Circuit's decision:

> [P]ermits the SEC to simply characterize alleged illegal trading as an "affirmative misrepresentation" whenever it cannot adequately establish the existence of a fiduciary relationship. Historically, the fiduciary-relationship element has required the SEC to meet exacting pleading standards; now, regulators have license to charge many acts of garden-variety fraud or financial unfairness under the nebulous rubric of "affirmative misrepresentation." Conceivably, that could embrace any fraud involving the purchase or sale of securities, not merely the prototypical Section 10(b) charge where insiders exploit inside information for personal advantage as a normal emolument of corporate office.

Id. (citation omitted).

made available."[154] While a false statement to a computer may be deemed material in that the user would be denied access if they used their true identity, it does not meet the 10b-5 standard because the false statement does not affect investor decision making. The fact that the information Dorozhko stole met this definition of material is irrelevant. To meet the materiality requirement in the computer hacking context, the Court would need to broaden the definition of materiality to encompass any material misrepresentation made in connection with a securities transaction. Currently, the law appears to extend only to material misrepresentations made to the investing public.

Again, the same issue arises with the element of reliance. Reliance is a required element of a Section 10(b) action because it establishes the causal connection between the misrepresentation and the economic injury; in other words, but for the misrepresentation, the investor would have refrained from entering a securities transaction.[155] The misrepresentation need not be the sole cause, but a substantial or significant one.[156] In the securities context, a court determines whether the investor relied on an affirmative misrepresentation by weighing several factors:

> (1) The sophistication and expertise of the plaintiff in financial and securities matters; (2) the existence of long standing business or personal relationships; (3) access to relevant information; (4) the existence of a fiduciary relationship; (5) concealment of the fraud; (6) the opportunity to detect fraud; (7) whether the plaintiff initiated the stock transaction or sought to expedite the transaction; and (8) the specificity or generality of the misrepresentations.[157]

Recognizing that direct proof of reliance is oftentimes an irrelevant and unreasonable evidentiary burden,[158] the Court adopted the fraud on

154. Basic Inc. v. Levinson, 485 U.S. 224, 231–32 (1988) (quoting TSC Indus., Inc. v. Northway, Inc., 426 U.S. 438, 449 (1976)). In other words, if the nonpublic information would affect the company's stock price, the information would be material.

155. *Id.* at 243. In the section 10(b) context, reliance is coterminous with causation in fact. Wilson v. Comtech Telecomm. Corp., 648 F.2d 88, 92 & n.7 (2d Cir. 1981).

156. *Wilson*, 648 F.2d at 92.

157. Kennedy v. Josephthal & Co., 814 F.2d 798, 804 (1st Cir. 1987) (quoting Zobrist v. Coal-X, Inc., 708 F.2d 1511, 1516–17 (10th Cir. 1983)).

158. In *Blackie v. Barrack*, 524 F.2d 891, 907 (9th Cir. 1975), the Ninth Circuit eliminated the direct reliance requirement. It explained:

the market theory of reliance.[159] This theory assumes that stock prices are determined by an investor's evaluation of publicly available material information; therefore, any material misrepresentation will alter the stock price, effectively defrauding investors who rely on price as an indication of the stock's value.[160] A computer relying on a false identification does not fall within 10b-5's understanding of reliance because the hacker's misrepresentation is made to a computer, not an investor. In the securities law context, it is reliance on the part of the investor that matters. In the computer hacker context, at most, the investor relies on any distortion in price caused by the hacker's subsequent trade. It is a stretch to say that but for the computer hack, the investor would not have engaged in a securities transaction. The link between the affirmative misrepresentation and reliance by the investor is a step removed. For Section 10(b) and Rule 10b-5 to apply courts would need to fashion a theory of reliance that bridged the gap between the misrepresentation and investor's reliance.

> A purchaser on the stock exchanges may be either unaware of a specific false representation, or may not directly rely on it; he may purchase because of a favorable price trend, price earnings ratio, or some other factor. Nevertheless, he relies generally on the supposition that the market price is validly set and that no unsuspected manipulation has artificially inflated the price, and thus indirectly on the truth of the representations underlying the stock price—whether he is aware of it or not, the price he pays reflects material misrepresentations. Requiring direct proof from each purchaser that he relied on a particular representation when purchasing would defeat recovery by those whose reliance was indirect, despite the fact that the causational chain is broken only if the purchaser would have purchased the stock even had he known of the misrepresentation.

Id. at 907.

159. *Basic Inc.*, 485 U.S. at 241–43.

160. Peil v. Speiser, 806 F.2d 1154, 1160–61 (3d Cir. 1986). In *Peil*, the court stated:

> The causal connection between the defendants' fraud and the plaintiffs' purchase of stock in such a case is no less significant than in a case of direct reliance on misrepresentations. In both cases, defendants' fraudulent statements or omissions cause plaintiffs to purchase stock they would not have purchased absent defendants' misstatements and/or omissions.

Id.

2. Problems With Timing and the "in Connection With" Requirement

Though easier to overcome, issues of timing arise with regard to the statute's second element: the "in connection with" requirement. Whether computer hacking for purposes of obtaining nonpublic information is sufficiently "in connection with" the purchase or sale of securities to fall under Section 10(b) depends largely on how a court characterizes the fraudulent act. The SEC interprets the phrase broadly, but not "so broadly as to convert every common law fraud that happens to involves securities into a violation of 10(b). Section 10(b) requires "deception 'in connection with the purchase or sale of any security,' not deception of an identifiable purchaser or seller."[161] The general rule is that the "scheme to defraud and the sale of securities coincide[;]" however its application is far from clear.[162]

In *O'Hagan*, the court construed the "in connection with" requirement within the context of its newly adopted misappropriation theory. Recognizing that nonpublic information is property to which a company is entitled exclusive use, the Court reasoned that "fraud is consummated, not when the fiduciary gains the confidential information, but [rather] when . . . the information [is used] to purchase or sell securities."[163] This hurdle is necessary because, in a misappropriation on the source case, receipt of nonpublic information is not fraudulent; rather it is the investor's later breach of his fiduciary duty to his source. Therefore, "[t]he securities transaction and the breach of duty . . . coincide."[164] The securities transaction and the breach of duty would not coincide, however, if the property obtained through fraudulent means had independent value—that is, the property could be used for any number of transaction unrelated to the securities market.[165]

161. United States v. O'Hagan, 521 U.S. 642, 658 (1997).

162. SEC v. Zandford, 535 U.S. 813, 822 (2002).

163. *O'Hagan*, 521 U.S. at 656.

164. *Id.* at 656.

165. The government conceded that embezzling funds to finance a security trade, while fraudulent, is not "in connection with" the purchase or sale of securities, because the misappropriated funds have independent value—that is, the funds could be used for any number of transactions unrelated to the securities market. Therefore, a subsequent securities trade would be sufficiently detached from the "in connection with" requirement. Misappropriation of nonpublic information, on the other hand, derives its value solely from its utility in securities trading. *Id.* This discussion appeared as dicta, so it was initially unclear whether the Court intended to introduce a requirement that the property obtained have no independent value. However, five years later, the Court in *SEC v. Zandford* stated that it did not "read *O'Hagan* as so limited." *Zandford*, 535 U.S. at 824. This reading makes sense because it is counterintuitive to draw lines based on possible alternative uses of property when it is clear from the facts that the investor obtained the information with but one

This distinction is of little concern here because the Court accepted that misappropriated nonpublic information had no value apart from its utility in securities trading.

Affirmative misrepresentation cases, however, are different. Here, the fraudulent act is the misrepresentation itself—no subsequent conduct is necessary to consummate the fraud.[166] On the other hand, in Dorozhko's case, the hack and subsequent securities transaction took place only thirty minutes apart, arguably as part of one single scheme to defraud.[167] If characterized as a single scheme, the fraud would not be complete until the securities transaction was complete; if Dorozhko chose not to engage in a securities transaction, his hack would not trigger Section 10(b) and Rule 10b-5. Borrowing the Court's language in *O'Hagan*, Dorozhko's "fraud [was] consummated not when [he] gain[ed] the confidential information, but when . . . he use[d] the information to purchase [and] sell securities. [Dorozhko's] securities transaction and the breach of [the computer's secure network] thus coincide."[168] The intent underlying the Section 10(b) and Rule 10b-5 prohibition supports the single scheme viewpoint because the ultimate securities transaction affects the integrity of the market the same way insider trading would.[169]

A single scheme approach is also supported by the Court's decision in *United States v. Zandford*, which couched the "in connection with" requirement in terms of independent events.[170] In *Zandford*, a securities broker persuaded a client to grant him a power of attorney allowing him to engage in securities transactions without prior approval.[171] Using this power, the broker then sold his client's securities and embezzled the proceeds.[172] The Court deemed this "scheme" deceptive because "each [sale] was neither authorized by, nor disclosed to, the [client]. . . . Each time [Zandford] exercised his power of disposition for his own benefit, that conduct, without more, was a fraud."[173] The Court determined that Zandford's fraud and sales were not independent events; rather the

intent—to use that information as a basis for his securities transaction.

166. *See O'Hagan*, 521 U.S. at 656.

167. SEC v. Dorozhko, 606 F. Supp. 2d 321, 329 (S.D.N.Y. 2008) *rev'd,* SEC v. Dorozhko, 574 F.3d 42 (2nd Cir. 2009).

168. *O'Hagan*, 521 U.S. at 656.

169. *See id.* at 685–869 (Stevens, J. dissenting).

170. *See Zandford*, 535 U.S. at 820–21.

171. *Id.* at 815.

172. *Id.* at 821.

173. *Id.* at 820–821 (internal citations omitted).

fraud coincided with the sales themselves.[174] Arguably, Dorozkho's fraud coincided with his later purchase and sale of securities because the hack and subsequent transaction were not independent events. That Dorozhko's hack and subsequent trade occurred only thirty minutes apart indicates that hack was designed to acquire nonpublic information that would inform his securities transactions.

With two logical and competing arguments construing the "in connection requirement," it is hardly clear how the Court would decide the issue. Although there is a strong argument that Dorozhko's hack and trade was one deceptive scheme, it is equally plausible that the Court would deem the fraud consummated by the misrepresentation itself.

VI. HISTORY AND GOOD PUBLIC POLICY SUPPORTS CONDEMNATION OF COMPUTER HACKING IN CONNECTION WITH SECURITIES TRANSACTIONS UNDER SECTION 10(B) AND RULE 10B-5.

Focusing insider trading liability on a fiduciary duty has created a gap in enforcement that makes trades based on lawfully obtained nonpublic information illegal and trades based on unlawfully obtained nonpublic information legal.[175] This anomalous result makes little sense. Therefore, although the Second Circuit's newly derived theory of insider trading liability does not comport with current securities law,[176] history and good policy favors a finding that computer hacking is in fact deceptive under Section 10(b) and Rule 10b-5. Such policy considerations include (1) the original intent of the securities laws, (2) economic efficiency, (3) moral considerations of fairness, (4) implied congressional consent, and most importantly (5) more appropriate punishment and remedies.

A. Original Intent of the Securities Laws

First, in promulgating Section 10(b) and Rule 10-b5, Congress did not intend to delineate specific acts or practices that constitute fraud. Rather, the laws were "designed to encompass the infinite variety of devices by which undue advantage may be taken of investors and others."[177] Thus, "[c]onduct by a defendant that had the principal purpose and effect of creating a false appearance in deceptive

174. *Id.* at 820.
175. Wheatley, *supra* note 141, at 51.
176. *See generally* Bainbridge, *supra* note 129, at 1.
177. *In re* Cady, Roberts & Co., 40 S.E.C. 907, 911 (1961).

transactions as part of a scheme to defraud is conduct that uses or employs a deceptive device within the meaning of Section 10(b)."[178] Nowhere does Section 10(b) or Rule 10b-5 premise "deception" on the existence of a fiduciary duty.[179] Furthermore, Section 10(b) was intended to prohibit invention of any other "cunning devices,"[180] suggesting that the courts should tailor the laws to capture innovations not contemplated when the Securities Act was passed. This would include trading made possible by computer hacking.

Moreover, in 1987, the Senate proposed a bill, the Insider Trading Proscriptions Act (ITP Act) for consideration by Congress.[181] The Act proposed a statutory definition of insider trading which would have prohibited:

> [T]rading while in possession of material, nonpublic information . . . if such information has been obtained by, or its use would constitute, directly or indirectly, (A) theft, bribery, misrepresentation, espionage (through electronic or other means) or (B) conversion, misappropriation, or a breach of any fiduciary duty, any personal or other relationship of trust and confidence, or any contractual or employment relationship.[182]

Under this language, computer hacking would be illegal insider trading as theft or espionage through electronic means. Although Congress ultimately elected not to pass the ITP Act, it was not because the senate objected to the types of conduct included in the definition.[183] Rather, Congress chose to leave the task of identifying insider trading to the judiciary, reasoning that "the court-drawn parameters of insider trading have established clear guidelines for the vast majority of traditional insider trading cases, and . . . a statutory definition could potentially be narrowing, and in an unintended manner facilitate schemes to evade the law."[184] Notwithstanding the abandonment of the

---

178. Simpson v. AOL Time Warner Inc., 452 F.3d 1040, 1052 (9th Cir. 2006).

179. *See* 15 U.S.C. § 78j(b) (2006).

180. *Stock Exchange Regulatory Hearing on H.R. 7852 & 8720 Before the H. Comm. on Interstate and Foreign Commerce*, 73d Cong. 115 (1934) (statement of Thomas Corcoran, Counsel with the Reconstruction Finance Corporation).

181. Insider Trading Sanctions Act, Pub. L. No. 100-704, 102 Stat. 4677, 11–13 (1988).

182. Donna M. Nagy, *Insider Trading and the Gradual Demise of Fiduciary Principles*, 94 IOWA L. REV. 1315, 1368 (2009).

183. *Id.*

184. *Id.* (citation omitted).

ITP Act, it is clear that Congress believes that insider trading law should reach trades based on nonpublic information acquired through computer hacking.

B. Economic Efficiency

One goal of Section 10(b) and Rule 10b-5, oft repeated, is the need to protect the integrity of the securities markets from abuses by those with access to material nonpublic information that would affect the price of the corporation's securities upon public disclosure.[185] The "integrity of the market" rationale for banning insider trading thus relies on the notion that proper stock valuation can be made only when factors motivating an investor's trade are available to the public.[186] If such factors were unavailable to the outsider, he would theoretically buy or sell at the wrong price, resulting in a net loss.[187] It follows that eliminating insider trading would increase investor confidence that they are not trading at an informational disadvantage. Because the securities market is the backbone of the American commercial system, integrity of the market is essential;[188] and conduct that threatens market integrity, such as computer hacking, should therefore violate Section 10(b) and Rule 10b-5.

---

185. United States v. O'Hagan, 521 U.S. 642, 653 (1997) (stating that the purpose of the Securities Act was "to insure honest securities markets and thereby promote investor confidence"); SEC v. Texas Gulf Sulphur Co., 401 F.2d 833, 852 (2d Cir. 1968) ("It was the intent of Congress that all members of the investing public should be subject to identical market risks, [which include] the risk that one's evaluative capacity . . . may exceed another's capacity.").

186. *See* Basic Inc. v. Levinson, 485 U.S. 224, 245, 247 (1988).

187. BAINBRIDGE, *supra* note 23, at 149–150. Professor Bainbridge argues that this reasoning is flawed because it assumes that outsiders trade only with insiders making trades based on nonpublic information. Given the impersonal nature of the securities exchange, gains will be shared by insiders with knowledge of material nonpublic information and outsiders with no such knowledge. *Id.* at 150–51.

188. *Illegal Insider Trading: How Widespread Is the Problem and Is There Adequate Criminal Enforcement?: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. 1–2 (2006) (statement of Arlen Specter, Senator, State of Pennsylvania). However, some argue that deregulating insider trading would benefit both society and the firm. *See generally* HENRY G. MANNE, INSIDER TRADING AND THE STOCK MARKET (1966). First, insider trading would allow for a more efficient market because the market price of a company's securities would be set at the level it would receive if the nonpublic information were publicly available. For example, if a share is selling at $30, but knowledge of material nonpublic information would cause the price to rise to $40, insider trading would cause the price to reach $40 earlier—in other words, before the information is made public. *Id.* at 77–91. Second, insider trading would serve as an efficient way of compensating and incentivizing entrepreneurs to innovate. *Id.* at 131–41. This second argument, however, seems to ignore the fact that insiders often trade on negative nonpublic information to avoid losses.

C. Moral Rationale

Allowing theft of nonpublic information committed for the sole purpose of trading on that information flies in the face of morality. Justice Blackmun, in his *Chiarella* minority opinion, noted that the most "dramatic evidence" of Chiarella's fraud was the fact that he stole information for personal benefit knowing that it was wrong and forbidden by his employer.[189] After all, "[t]he more unfair the activity, the more justification there is for regulation."[190] Securities trading should be free from investors having any undue advantages.[191] Thus, material nonpublic information should not be used for the personal benefit of anyone because such use would be inherently unfair to outside investors.[192] This is particularly true when the information is accessed through unlawful means such as computer fraud. Despite being a non-fiduciary, arguably, the computer hacker's conduct is more reprehensible because the he takes affirmative action to not only use undue advantage in securities trading, but to also break state and federal computer fraud laws.

D. Implied Congressional Consent

Congress has opted not to pass legislation limiting the reach of insider trading laws to transactions made in breach of a fiduciary duty. While the question of whether a computer hacker, who owes no fiduciary duty to either the shareholders of a corporation or the source of confidential information, may be liable for insider trading under Rule 10b-5 was one of first impression for the Second Circuit, it was not the first instance where the SEC prosecuted a computer hacker.[193] In 2005 and 2007, the SEC successfully sought a temporary restraining order to freeze the defendants' assets and an order to repatriate funds taken outside of the United States.[194] Both cases were factually similar to

---

189. Chiarella v. United States, 455 U.S. 222, 245–46 (1980) (Blackmun, J., concurring).

190. Prentice, *supra* note 11, at 305.

191. *Chiarella*, 455 U.S. at 241 (Burger, C.J., dissenting).

192. *Id.* at 241 (citing *In re* Cady, Roberts & Co., 40 S.E.C. 907, 912 (1961)).

193. In Blue Bottle Limited., Litig. Release No. 20018, 90 SEC Docket 268 (Feb. 26, 2007), the defendants were charged with illegally accessing, through a computer system, information about imminent new releases. Using that information, the defendants traded in the securities of twelve corporations prior to public dissemination, realizing $2,707,177 in profits. In Lohmus Haavel & Viisemann, Litig. Release No. 19450, 86 SEC Docket 1591 (Nov. 1, 2005), the defendants were charged "with conducting a fraudulent scheme involving the electronic theft and trading in advance of more than 360 confidential press releases issued by more than 200 U.S. public companies," realizing at least $7.8 million in illegal profits.

194. Blue Bottle Ltd., 90 SEC Docket at 268; Lohmus Haavel & Viisemann, 86 SEC

Dorozhko.[195] Although each judge granted the SEC's requested relief, neither issued a published opinion.[196] Congress has implied its approval of such decisions by continuing to take no action in defining insider trading under federal law.

E. Criminal Computer Fraud Penalties Are Insufficient

Criminal penalties for computer fraud are insufficient where the misappropriated information is used to trade in securities. First, under the federal computer fraud statute, a hacker would be subject only to a fine and a term of imprisonment.[197] Computer fraud statutes do not provide means for freezing assets or repatriating profits made by foreign defendants.[198] In contrast, under the Securities Act, the SEC is able to seek injunctive relief to prevent future unlawful trading, asset freezes, disgorgement of illegally obtained proceeds, and civil penalties of up to three times the illegal profits made or the losses avoided.[199] It may also seek criminal penalties, including imprisonment, where the selling or buying of securities was willful and fraudulent.[200] As SEC Enforcement Deputy Director Peter Bresnan points out, "In today's global economy, where con artists can misuse computer technology to defraud innocent U.S. investors from far beyond our borders, freezing the unlawful profits of those behind these intrusion schemes is especially important."[201] Second, despite the availability of a private cause of action against hackers, companies are reluctant to pursue such cases for fear of the negative publicity that accompanies public disclosure of such security

Docket at 1591.

195. *See supra* note 194 and accompanying text.

196. *Id.*

197. 18 U.S.C. § 1030(a)–(c) (2006).

198. *See id.* § 1030.

199. 15 U.S.C. §§ 78u(d)(1), 78u-1, 78u-2. Prior to 1984, inside traders were only subject to disgorgement and possibly criminal sanctions. Civil penalties could not be imposed until the defendant was convicted criminally. NASSER ARSHADI & THOMAS H. EYSSELL, THE LAW AND FINANCE OF CORPORATE INSIDER TRADING: THEORY AND EVIDENCE 49 (1993). This punishment provided little deterrent value. So, in 1984, Congress passed the Insider Trading Sanctions Act of 1984, 98 Stat. 1264 (1984) (codified at 15 U.S.C. § 78), which increased criminal fines and prison times and allowed the SEC to impose treble damages.

200. 15 U.S.C. § 78u(c), 78u-2. Finally, the SEC is authorized to make "bounty" payments to any person who provides information leading to civil penalties. The bounty awarded may be up to 10% of the civil penalty collected. *Id.* §§ 78u-1.

201. Press Release, SEC, SEC Obtains Order Freezing $3 Million in Proceeds of Suspected Foreign-Based Account Intrusion Scheme (Mar., 7, 2007) (on file with author), *available at* http://www.sec.gov/news/press/2007/2007-33.htm.

breaches.[202] This is particularly true where the security breach does not result in significant financial losses.[203]

Increased penalties serve as a better deterrent and more appropriate punishment.[204] To illustrate, the SEC oftentimes charges a defendant with securities fraud under Rule 10b-5 even where it has already obtained a computer hacking or wire fraud conviction. In *SEC v. Zandford*, the defendant was indicted and later convicted of thirteen counts of wire fraud in violation of 18 U.S.C. § 1343.[205] His punishment consisted of fifty-two months in prison and payment of $10,800 in restitution.[206] After the indictment, the SEC filed a civil suit alleging that Zandford also violated Section 10(b) and Rule 10b-5 by engaging in a scheme to defraud. Zandford was found guilty, and as a result, was enjoined from engaging in future violations of the securities laws and ordered to disgorge the $343,000 he realized in ill-gotten gains.[207] Had Section 10(b) been unavailable, Zandford would have retained the fruit of his crime.

VII. Arguing Fidelity to Chief Justice Burger's Fraud on the Investor Theory of Insider Trading

Because the newly created affirmative misrepresentation theory cannot be sustained and computer hacking does not fit within the contours of classical insider trading or the fraud on the source theory adopted by the Supreme Court in *O'Hagan*, the Court or Congress must adopt a new version of the misappropriation theory or an entirely new theory of insider trading to capture this type of deceptive theft. Legal scholars have advocated several approaches including the parity of information theory, property rights theory, deceptive acquisition theory, and the fraud on investors theory. This section will discuss each briefly, and then propose the fraud on investors theory as the superior solution.

---

202. Wheatley, *supra* note 141, at 55–56.

203. *Id.*

204. Admittedly, Congress could achieve the same result by revising the computer fraud statute to add disgorgement, asset freezes, and injunctive relief as available remedies.

205. SEC v. Zandford, 535 U.S. 813, 815–16 (2002).

206. *Id.* at 816.

207. *Id.*

A. Parity of Information Theory

The parity of information theory would prohibit trading on all nonpublic material regardless of the manner in which the investor gained access to such information. However, this theory has been repeatedly rejected by the Supreme Court on the grounds that it would inhibit legitimate activities conducted by market analysts such as questioning corporate officers and "ferret[ing] out and analyz[ing] information."[208] Such inhibition would negatively affect market efficiency in stock pricing, to the detriment of all investors. Because this theory has been foreclosed by the Court, adoption would require congressional action.

B. Property Rights Theory

The property rights theory finds its basis in *In re Cady, Roberts & Co.*, which based liability on the misuse of "information intended to be available only for a corporate purpose and not for the personal benefit of anyone."[209] Recognizing that nonpublic information is "property" to which companies have exclusive use, a property rights approach would make illegal trades made by an investor who uses, for his personal benefit, material nonpublic information intended by the company to be used only for a corporate purpose.[210] By eliminating the fiduciary duty requirement, this rule would capture illegal conduct such as computer hacking because the information obtained through hacking would be used for the hacker's personal benefit rather than for a corporate purpose.[211] Moreover, this theory would eliminate a misappropriator's ability to escape liability my disclosing his intent to trade on nonpublic information to his source.

The property rights theory, however, may prove overly broad, resulting in over-enforcement.[212] For example, depending on the characterization of "personal benefit" and corporate purpose, a property rights approach may inhibit the legitimate activities of market analysts. Moreover, this approach may foreclose trading based on nonpublic information gained through superior skill or effort.

---

208. Dirks v. SEC, 463 U.S. 646, 658–59 (1983).
209. *In re* Cady, Roberts & Co., 40 S.E.C. 907, 912 (1961).
210. Wheatley, *supra* note 141, at 53–54.
211. *Id.*
212. Wheatley, *supra* note 141, at 54.

C. Deceptive Acquisition Theory

The "deceptive acquisition" theory has been proposed as an alternative to the classical and misappropriation theories on insider trading.[213] This theory would make any person who acquired nonpublic information through deceptive means liable under Section 10(b) and Rule 10b-5, in the absence of a fiduciary relationship. Donna M. Nagy, Professor of Law at the Indiana University Maurer School of Law, a proponent of this theory, points out that despite the Supreme Court's focus on a fiduciary relationship, the plain language of the statute contains no such limitation and instead captures all deceptive devices used in connection with securities trading. Nagy argues that *Stoneridge Investment Partner, LLC v. Scientific-Atlanta, Inc.*, supported the "deceptive acquisition" theory when it recognized conduct itself could be deceptive under Section 10(b) and Rule 10b-5.[214] Deceptive devices are not limited to misstatements or omissions made by those with a duty to disclose.[215] To that end, computer hacking could be considered deceptive conduct in and of itself, despite the fact that the hacker lacked a preexisting fiduciary duty to the source.[216] This theory addresses Justice Blackmun's chief concern in *Chiarella*—that the Court failed to adequately consider the fact that Chiarella accessed nonpublic information that no honest investor could likewise access by legal means—because it reaches all scenarios where an investor capitalizes on nonpublic information gained solely through deceptive means.[217]

There are limits to the deceptive acquisition theory. First, it leaves untouchable those investors who obtain nonpublic information through outright theft, because theft lacks the requisite deception.[218] Second, the deceptive acquisition theory would not prevent a misappropriator from escaping liability by disclosing to his source his intent to trade, because such disclosure eliminates any deception.

---

213. Nagy, *supra* note 182, at 1369–70.

214. *Id.* at 1370 (discussing Stoneridge Inv. Partners, LLC. v. Scientific-Atlanta, Inc., 552 U.S. 148, 158 (2008)).

215. *Id.* at 1369–70.

216. *Id.* at 1370.

217. Chiarella v. United States, 445 U.S. 222, 247 (1980).

218. Nagy, *supra* note 182, at 1372.

D. Fraud on the Investors Theory

The fraud on the investors theory was espoused by Chief Justice Burger in his dissenting opinion in *Chiarella*. The theory prohibits all trades based on nonpublic information obtained through illegal means. Burger recognized that in the absence of a fiduciary duty, neither party to the business transaction has a duty to disclose information unknown to the other side. The policy underlying this rule breaks down, however, where such information was obtained by illegal or deceptive means. In other words, Section 10(b) and Rule 10b-5 should extend to *any* person who misappropriates material nonpublic information for the purposes of securities trading.[219] A duty to abstain or disclose would thus arise even when the misappropriator owed no fiduciary duty to shareholders or the source.[220]

The fraud on the investors theory of misappropriation is superior to the aforementioned theories as well as the fraud on the source theory currently followed for several reasons. First, by premising liability on access through unlawful means, the fraud on investors theory captures all forms of misappropriation, including deceptive theft and mere theft. Second, the fraud on investors theory eliminates timing issues involving the "in connection with" requirement.[221] By eliminating the breach of fiduciary duty requirement, the illegal conduct need not coincide with the securities transaction.[222] Instead, the deceptive device occurs when the defendant fails to disclose the nonpublic information on which he trades to the other parties of a securities transaction.[223] Third, the fraud on the investors theory better addresses the policies underlying the Section 10(b) prohibition. The fraud on the investors theory is premised on the idea that misappropriation, no matter its form, defrauds marketplace traders[224] and serves no useful function other than self-enrichment at the expense of others.[225] The best way to guarantee

---

219. *Chiarella*, 455 U.S. at 240 (Burger, C.J., dissenting). Section 10(b)'s broad language, which reaches *any* person in *any* fraudulent scheme, supports this reading by suggesting that congressional concern was not limited to trading by corporate insiders. *Id.* at 240–41 (emphasis added).

220. *See id.*

221. Nagy, *supra* note 100, at 1300.

222. *Id*.

223. *Id.*

224. Nagy, *supra* note 182, at 1373 (stating that "it is insider trading's impact on the securities market and the confidence of investors that provides the rationale for the Rule 10b-5 prohibition").

225. *Chiarella*, 455 U.S. at 241 (Burger, C.J. dissenting). Section 10(b)'s legislative history shows that Congress intended section 10(b) to prohibit "those manipulative and

integrity of the stock markets is to eliminate all trading based on misappropriated nonpublic information. Lack of a fiduciary duty does not change the harm done to market integrity and therefore should not be a requisite element of an insider trading case. Fourth, the fraud on the investor theory does not reach legitimate trading activities because informational advantages obtained through legal channels would not trigger a duty to disclose.[226]

Finally, Supreme Court precedent does not foreclose adoption of the fraud on the investor theory. In *Chiarella*, the Court rejected only the parity of information approach, noting that the government did not propose the misappropriation theory in its initial appeal. And in *Dirks*, the defendant did not misappropriate nonpublic information nor breach a duty of confidentiality. Finally, in *O'Hagan*, the Court limited its analysis to the fraud on the source theory of misappropriation proposed by the government. The Court did not expressly reject the broader fraud on the investor theory, leaving open the possibility that it adopt the theory in the future—much like the *Chiarella* Court did when it limited its analysis to the narrower theory argued before it.[227]

VIII. CONCLUSION

The Second Circuit's holding in *Dorozkho* reached a proper end through improper means by effectively combining two distinct theories of Section 10(b) liability into one. It is likely that a case applying the affirmative misrepresentation theory of insider trading laid out in *Dorozhko* will reach the Supreme Court on appeal in the near future. When such a time comes, the Court should reject this newly created theory in favor of the fraud on the investors theory originally proposed by Chief Justice Burger in *Chiarella*.

One could argue that insider trading liability should not be extended to computer hackers by the judiciary. However, this ignores the fact that all insider trading law, including the classical theory and "fraud on the source" theory, has been judicially created and that "Section 10(b) was designed as a catchall clause to prevent fraudulent practices."[228]

---

deceptive practices which have been demonstrated to fulfill no useful function. S. REP. NO. 73-792, at 6 (1934).

226. Nagy, *supra* note 100, at 1303–1304.

227. United States v. O'Hagan, 521 U.S. 642, 655 n.6 (1997). The Court did not consider the broader theory proposed by Chief Justice Burger in *Chiarella* because the government did not choose to advance such a theory and rather premised its argument on disclosure obligations to the source of the information. *See id.* at 652.

228. *Chiarella*, 455 U.S. at 226.

Given the courts' role in defining insider trading, the statute's plain text, and the SEC's policy goals, the Supreme Court should be permitted to broaden the scope of insider trading liability to capture unlawful conduct, such as computer hacking, despite lack of a disclosure duty. "The genius of insider trading law . . . is its flexibility, its ability to accommodate changing business practices, conditions and situations."[229] The Court must continue to interpret Section 10(b) and Rule 10b-5 to meet new challenges in maintaining the integrity of the securities markets.

The bottom line is that thieves are as culpable as the fiduciary and should be subject to insider trading laws just the same—to maintain the integrity of the stock market, eliminate unfairness, and deter future illegal conduct.

ELIZABETH A. ODIAN*

229. Linda Chatman Thomsen, Dir., Div. of Enforcement, SEC, Speech by SEC Staff: Remarks Before the Australian Securities and Investments Commission 2008 Summer School: U.S. Experience of Insider Trading Enforcement (Feb. 19, 2008).

* J.D. 2011, Marquette University Law School. The author would like to thank Professor Fallone for his insight and the staff of *Marquette Law Review* staff for their work on this piece.