HACKING WALL STREET: RECONCEPTUALIZING INSIDER TRADING LAW FOR COMPUTER HACKING AND TRADING SCHEMES

Kenneth Geisler II

ABSTRACT

This paper explores how insider trading law addresses computer hackers who employ cyberattacks in connection with the purchase or sale of securities. Current securities law is ill-equipped to deal with such hackers because, unlike the typical defendants in insider trading cases, hackers owe no fiduciary duty to shareholders and no duty of confidentiality to insiders that provide material non-public information. In order to bring hacker-traders within the ambit of federal securities law, the U.S. Securities and Exchange Commission (SEC) has relied on a novel theory of liability that treats hacking and trading as a form of deception in violation of Section 10(b) of the Securities Exchange Act of 1934. However, the viability of the SEC's theory remains to be seen as only one decision has endorsed it—*SEC v. Dorozhko*, 574 F.3d 42 (2d Cir. 2009). This paper argues that, from a normative perspective, the Second Circuit correctly expanded Section 10(b) to hacking and trading. However, this paper takes issue with the Second Circuit's proposition that hacking amounts to deception only when the hacker misrepresents his or her "identity in order to gain access to information that is otherwise off limits, and then steal[s] that information" for purposes of securities trading.

Currently, there is little scholarship that thoroughly explores the potential for hackers to use innovative cyberattacks in order to avoid liability for securities fraud. This paper adds to the existing literature by arguing that even if the judiciary were to adopt the SEC's reconceptualization of insider trading, it is unlikely that the theory would apply to certain sophisticated cybersecurity schemes—such as informed cyber-trading, whereby investors trade "on the basis of advanced knowledge of a cybersecurity breach." In addition, it is unlikely that *Dorozhko* would apply to schemes in which a group of hackers short a corporation's stock and then initiate a cyberattack, such as a distributed denial of service (DDoS) attack, in order to cause a decline in the stock price. Such conduct would not amount to "deceptive hacking" under *Dorozhko* because even though the hackers masqueraded their identities, they did not do so in order to obtain the type of confidential information typically at issue in illegal insider trading schemes.

TABLE OF CONTENTS

INTRODUCTION

A new breed of securities fraudsters are increasingly finding themselves in the crosshairs of the U.S. Securities and Exchange Commission (SEC). They commit their schemes in the high-tech environs of the internet, beyond the confines of the corporate boardroom and boiler room. They are criminal computer hackers who infiltrate the computer networks of corporations, law firms, and business newswires in order to obtain material non-public information and gain an edge in the markets.[1] "You don't need to be a Wall Street insider to pull off insider trading anymore."[2]

In response, the SEC has crafted a novel theory of insider trading in order to bring hackers within the scope of Section 10(b) of the Securities Exchange Act of 1934. But computer hackers who hack their way to confidential information for purposes of securities trading are unlike the typical insider trading defendant. Insider trading cases have largely been limited to two situations, each involving a different theory of liability:

---

[1] *See, e.g.*, U.S. SEC. & EXCH. COMM'N, *SEC Cybersecurity Roundtable* 6 (Mar. 26, 2014) ("Cyber incidents appear to be escalating in frequency, duration, and complexity."). In addition to corporations, law firms are increasingly targeted by hackers. "According to the ABA's 2017 *Legal Technology Survey Report*, 22% of responding firms had been breached—an increase of 8 percentage points from the previous year's survey." Mary Ellen Egan, *Cyberthreats 101: The Biggest Computer Crime Risks Lawyers Face*, ABA J. (Mar. 2018), http://www.abajournal.com/magazine/art.

[2] Ryan H. Gilinson, *Clicks and Tricks How Computer Hackers Avoid 10b-5 Liability*, 82 BROOK. L. REV. 1305, 1305 (2017).

(1) the classical theory, which applies to corporate insiders (employees of the company whose securities are the subject of the insider trading) who breach their fiduciary duty to the shareholders by trading in securities on the basis of non-public material information without first disclosing this information to the shareholders,[3] or

(2) the misappropriation theory, which applies to corporate outsiders (individuals who are not employed by the company whose securities are traded) who breach a duty of confidentiality by trading in securities on the basis of information that a source entrusted to them with the expectation that the outsider would not use the information for personal gain.[4]

Hackers who trade on the basis of information they obtained through hacking do not fit in either of these two categories. Hackers are corporate outsiders who owe no duty to shareholders and no duty to insiders who share information in trust.[5] Unlike a misappropriator, who exploits a relationship of trust in order to gain valuable information, hackers rely on their technical knowhow to obtain the information. In other words, "[a]lthough the hacker's advantage was [also] unfair, he garnered it not through privilege or special connections but through the much rarer combination of superior technologies, risk-taking, and criminal bravado."[6]

This paper explores the challenge in holding computer hackers liable for insider trading. It adds to the existing literature by arguing that even if the courts ultimately adopt the SEC's theory of insider trading, there would still remain the potential for innovative hackers to avoid liability. Part I provides an overview of the so-called classical and misappropriation theories of insider trading and briefly explains why the current legal framework is ill-equipped to deal with hackers.

Part II discusses the handful of SEC enforcement actions and Department of Justice (DOJ) criminal prosecutions brought against hackers, focusing in particular on two cases: *SEC v. Dorozhko*, in which the Second Circuit endorsed the SEC's theory of Section 10(b) liability for

---

[3] Corporate insiders include corporate directors, officers, employees, and other permanent insiders, as well as attorneys, accountants, consultants, and others who temporarily become fiduciaries of a corporation. United States v. O'Hagan, 521 U.S. 642, 652 (1997) (citing Dirks v. SEC, 463 U.S. 646, 655, n.14 (1983)).

[4] *See* United States v. O'Hagan, 521 U.S. 642, 652-53 (1997).

[5] While "[a]ttribution of cyber incidents is difficult," it is estimated that outsiders were responsible for 75% of recent cyber incidents and breaches, while internal actors caused 25%. White House Council of Economic Advisers, *The Cost of Malicious Cyber Activity to the U.S. Economy* 3 (Feb. 16, 2018), https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

[6] *See* Sung Hui Kim, *Insider Trading as Private Corruption*, 61 UCLA L. REV. 928, 998-1000 (2014) (explaining how hacking-trading is not conventional insider trading).

hackers who trade on the basis of information obtained from deceptive hacking techniques (i.e., "hacker-traders")[7]; and *SEC v. Dubovoy, et al.*, where the SEC and DOJ filed parallel actions against hackers who sold information they stole from business newswires to traders (i.e., "hacker-sellers"). These cases highlight the unique difficulties in bringing hacker-traders and hacker-sellers within the ambit of insider trading law.[8]

Part III briefly outlines some of the proposals for and against holding hackers liable for securities fraud. Part III argues that while the Second Circuit took the right step in *Dorozhko* by expanding Section 10(b) liability to hacker-traders, the court's definition of "deceptive hacking" unduly limits liability to hackers who trade on the basis of material non-public information. As a result, *Dorozhko* will be of little precedential value for future cases involving innovative cyberattacks that do not involve the theft of inside information, such as ransomware or distributed denial of service (DDoS) attacks intended to drive down the value of a company's stock. This paper concludes with a discussion of hypothetical cyberattacks that could pose problems for regulators and offers some potential solutions.

I. VULNERABILITIES IN CURRENT INSIDER TRADING LAW: WHY A NOVEL THEORY OF LIABILITY IS NEEDED FOR HACKING AND TRADING SCHEMES

The 1929 stock market crash was the catalyst for the Securities Exchange Act of 1934. Congress enacted the Exchange Act in order to "insure honest securities markets and thereby promote investor confidence."[9] Section 10(b) of the Exchange Act continues to serve as one of the government's primary tool against securities fraud. The statute makes it unlawful for any person, either directly or indirectly:

> To use or employ, in connection with the purchase or sale of any security . . . any manipulative or *deceptive* device or contrivance in contravention of such rules . . . as the [SEC] may prescribe as necessary or appropriate in the public interest or for the protection of investors.[10]

---

[7] *See* SEC v. Dorozhko, 574 F.3d 42 (2d Cir. 2009) (holding that hacking information for trading purposes could be actionable as insider trading securities fraud). *See also infra* Part II.A.
[8] *See* SEC v. Dubovoy et al., No. 15-cv-06076 (D.N.J. Aug. 10, 2015). *See infra* Part II.B.
[9] United States v. O'Hagan, 521 U.S. 642, 658 (1997); *See* Andrew Verstein, *Insider Trading in Commodities Markets*, 102 VA. L. REV. 447, 458 n.53 (2016) ("The degree to which Congress intended a broad insider trading prohibition is contested.").
[10] Securities Exchange Act of 1934, 15 U.S.C. § 78j(b) (emphasis added).

Pursuant to Section 10(b), the SEC promulgated Rule 10b-5.[11] Neither Section 10(b), Rule 10b-5, nor any other federal statute specifically addresses "insider trading."[12] Nevertheless, the federal courts relied on Section 10(b)'s proscription against "deceptive device[s]" in order to fashion two general theories of liability for insider trading—the classical and misappropriation theories.[13]

The classical (or traditional) theory was first recognized by the Supreme Court in *Chiarella v. United States*, 445 U.S. 222, 230 (1980).[14] The classical theory imposes Section 10(b) liability on a corporate insider who trades securities on the basis of non-public material information obtained through the course of the insider's employment without first disclosing the information to the shareholders.[15] Trading on the basis of such information is deemed to be "deceptive" because the corporate insider is placing his or her own welfare before the shareholders', thus breaching the insider's fiduciary duty owed to the shareholders.[16]

The misappropriation theory on the other hand, applies to a company outsider who personally profits from the use of confidential information entrusted to them without first informing the source of the information of their intent to trade on the information. These outsiders commit deception by breaching a duty of confidentiality owed to the source of

---

[11] Rule 10b-5 provides:

> 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,
> To employ any device, scheme, or artifice to defraud, [or]
> To make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading, or
> To engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person, in connection with the purchase or sale of any security.

17 C.F.R. § 240.10b-5 (2016). The scope of Rule 10b-5 is coextensive with Section 10(b); therefore, this paper uses Section 10(b) to refer to both the statutory provision and the Rule. *See* United States v. O'Hagan, 521 U.S. 642, 651 (1997) ("Liability under Rule 10b-5 . . . does not extend beyond conduct encompassed by § 10(b)'s prohibition.").

[12] *See* Sarah Baumgartel, *Privileging Professional Insider Trading*, 51 GA. L. REV. 71, 74 (2016); *see also* J. Kelly Strader, *(Re)conceptualizing Insider Trading United States v. Newman and the Intent to Defraud*, 80 BROOK. L. REV. 1419, 1427 (2015).

[13] Joshua Mitts & Eric L. Talley, *Informed Trading and Cybersecurity Breach*, Harv. Bus. L. Rev. 36 (2018) ("Under either classical or misappropriation theory, then, the insider-trading prohibition has come to be understood to mean that 'individuals may not purchase or sell securities based *on knowledge of nonpublic information that they legally obtained or possessed as a consequence of their employment or similar circumstances*.'")

[14] Chiarella v. United States, 445 U.S. 222, 230 (1980).

[15] *Id.* at 228.

[16] J. Kelly Strader, *(Re)conceptualizing Insider Trading United States v. Newman and the Intent to Defraud*, 80 BROOK. L. REV. 1419, 1428 (2015); United States v. Cusimano, 123 F.3d 83, 87 (2d Cir. 1997) (distinguishing "the traditional theory of insider trading" from "the misappropriation theory").

information.[17] While the outsider is not a corporate employee and thus owes no duty to the shareholders of the corporation, the outsider nevertheless owes a duty of confidentiality or loyalty to the source.[18] As one court has explained, "[i]n plain terms, when Sally tells Joe insider information about her corporation, to be held by Joe in confidence, and Joe then trades on that information without telling Sally, Joe is guilty of" deceiving Sally.[19]

The Supreme Court first recognized the misappropriation theory in *United States v. O'Hagan*, 521 U.S. 642 (1997).[20] There the defendant was employed by a law firm that represented a bidding company in a contemplated tender offer.[21] After learning of the proposed deal, the defendant lawyer purchased shares in the target company before the deal was made public.[22] Because the defendant's law firm represented the bidder, the defendant did not owe a fiduciary duty to the target company's stockholders and thus, the classical theory did not apply.[23] The Court held that he was still liable, reasoning that he had committed deception by feigning loyalty to his law firm and its client while secretly profiting from confidential information he obtained from them.[24]

In short, the classical and misappropriation theories rely on a breach of duty as a proxy for deception. As a result, they leave a gap for hackers to avoid Section 10(b) liability. The classical theory does not apply to hackers because hackers owe no fiduciary duty to the corporation's shareholders and are under no obligation to abstain from trading or disclosing the information.[25]

---

[17] United States v. Cusimano, 123 F.3d 83, 87 (2d Cir. 1997); *see also* Robert A. Horowitz & Geoffrey S. Berman, *Computer Hacking and Insider Trading Liability*, 31 No. 9 WESTLAW J. CORP. OFFICERS & DIRECTORS LIABILITY 1 (Nov. 2, 2015).

[18] "This fiduciary duty is breached when the corporate outsider does not disclose his knowledge of the information to its source and, subsequently, trades on the basis of that information." Brian A. Karol, *Deception Absent Duty: Computer Hackers & Section 10(B) Liability*, 19 U. MIAMI BUS. L. REV. 185, 194 (2011).

[19] United States v. McPhail, 831 F.3d 1, 4 (1st Cir. 2016).

[20] United States v. O'Hagan, 521 U.S. 642 (1997); *see* SEC v. Rocklage, 470 F.3d 1, 6 (1st Cir. 2006) (discussing the theoretical underpinnings of insider trading jurisprudence).

[21] *O'Hagan*, 521 U.S. at 647.

[22] *Id.* at 647-48.

[23] *Id.* at 653 n 5.

[24] *See id.* at 653-55. The Court noted in *O'Hagan* that it would make "scant sense to hold a lawyer like [the defendant] a § 10(b) violator if he work[ed] for a law firm representing the target of a tender offer, but not if he work[ed] for a law firm representing the bidder. The text of the statute requires no such result." *Id.* at 659.

[25] *See, e.g.*, John Reed Stark, *Guest Post: Think the SEC EDGAR Data Breach Involved Insider Trading? Think Again* (Oct. 2, 2017), https://www.dandodiary.com/2017/10/articles/cyber-liability/guest-post-think-sec-edgar-data-breach-involved-insider-trading-think/; Brian A. Karol, Note, *Deception Absent Duty: Computer Hackers & Section 10(B) Liability*, 19 U. MIAMI BUS. L. REV. 185, 193 (2011).

The misappropriation theory was designed for outsiders and is therefore more appropriate for hackers. However, it is also inapplicable because in the context of hacking the "'deception' usually relates directly to the . . . unauthorized computer access," not to the unauthorized use of information in violation of a relationship of trust.[26] In other words, the misappropriation theory does not encompass the illegal acquisition of information; rather "its essence is lawful possession, but illicit application."[27] Justice Ginsburg's language in *O'Hagan* ensured that the misappropriation theory would be limited by a breach of duty requirement.[28] Justice Ginsburg explained that a defendant is liable when he or she "misappropriates confidential information for securities trading purposes, in breach of a duty owed to the source of the information."[29]

Nevertheless, hacking and trading schemes pose many of the same problems as misappropriators. Specifically, the misappropriation theory was designed to "'protec[t] the integrity of the securities markets against abuses by 'outsiders' to a corporation who have access to confidential information that will affect the corporation's security price when revealed, but who owe no . . . duty to that corporation's shareholders.'"[30] The harm that the outsider-misappropriator causes to trading partners is similar to that caused by the hacker-trader insofar that when the hacker trades on information illegally obtained from computer networks, the hacker is "able to trade with unwitting market participants using an unfair advantage."[31] In both situations, the third-party "is trading at an informational disadvantage."[32] This information asymmetry partly explains why the SEC prohibits insider trading: it "undermines investor confidence in the fairness and integrity of the securities markets..."[33] The argument is that insider trading, if left unchecked, leads to a situation in which the "only trades left on the table for outsiders will be those that insiders have spurned because they offer a lower return than is

[26] Stark, *supra* note 25.
[27] Robert A. Prentice, *The Internet and Its Challenges for the Future of Insider Trading Regulation*, 12 HARV. J. L. & TECH. 263, 297 (1999).
[28] *Id.*
[29] *O'Hagan*, 521 U.S. at 652.
[30] *Id.* at 653.
[31] Adam R. Nelson, Note, *Extending Outsider Trading Liability to Thieves*, 80 FORDHAM L. REV. 2157, 2196 (2012).
[32] *Id.*
[33] U.S. SEC. & EXCH. COMM'N, *Insider Trading*, https://www.sec.gov/fast-answers/answersinsiderhtm.html (last visited April 9, 2018). "The legal version [of insider trading occurs] when corporate insiders—officers, directors, and employees—buy and sell stock in their own companies." *Id.*

available elsewhere."[34] Eventually, the disadvantaged outsiders will no longer invest in the markets, thereby reducing public ownership of corporations.[35]

However, hacking and trading does raise unique issues. Recent developments, such as the Equifax data breach, demonstrates that hacking and trading schemes can involve information typically not at issue in insider trading cases. For example, in March 2018, the SEC charged a former Equifax executive with insider trading, alleging that he sold nearly $1 million in company stock a week prior to the public announcement of the major data breach caused by hackers who stole personal data on 143 million consumers.[36] The theft of millions of Americans' personally identifiable information was valuable to identity thieves in the black market and knowledge of this data breach constituted valuable information for investors.[37] In comparison, the traditional insider trading case only involves the misuse of information that is only "valuable due to 'its utility in securities trading.'"[38]

The Equifax breach also demonstrates the possibility of novel hacking and trading schemes involving put options or short selling. In June 2018, DOJ charged a former Equifax software development manager with insider trading, alleging that he bought eighty-six put options in Equifax stock after learning of the data breach, resulting in a profit of $75,000.[39] Likewise, the Equifax hackers could have taken a short position in the stock, reasoning that news of their cyberattack would cause a plummet in stock price.[40] Holding such hackers liable for

---

[34] George W. Dent, *Why Legalized Insider Trading Would Be a Disaster*, 38 DEL. J. CORP. L. 247, 262 (2013).
[35] *Accord.* Brian A. Karol, Note, *Deception Absent Duty: Computer Hackers & Section 10(B) Liability*, 19 U. MIAMI BUS. L. REV. 185, 217 (2011) (arguing that the "harm to market integrity and investor confidence caused by computer hackers, . . . is of the same variety as the harm caused by those who legally obtain the information, but are liable under the classical and misappropriation theories of insider trading.").
[36] Complaint at 5, SEC v. Jun Ying, No.1:18-cv-01069-CAP (N.D. Ga. Mar. 14, 2018); *see* Stacy Cowley, *Ex-Equifax Executive Charged with Insider Trading Tied to '17 Breach*, N.Y. TIMES (Mar. 14, 2018).
[37] *See* Complaint at 13, SEC v. Jun Ying, No. 1:18-cv-01069-CAP (N.D. Ga. Mar. 14, 2018) (alleging defendant Equifax executive "knew . . . that the information that Equifax itself was the victim of a major cybersecurity breach was material and nonpublic, and [he] used that information when making [the] securities transactions."); *see also* United States v. Jun Ying, No. 1:18-CR-74-AT, 2018 WL 6322308, at *2 (N.D. Ga. Dec. 4, 2018) (rejecting defendant's arguments that the indictment did not allege that defendant knowingly possessed material nonpublic information and that he used such information when he traded).
[38] United States v. Falcone, 257 F.3d 226, 233–34 (2d Cir. 2001) ("*O'Hagan*'s [sic] requirement that the misappropriated information 'ordinarily' be valuable due to 'its utility in securities trading,' . . . appears to be a more generally applicable factor in determining whether section 10(b)'s 'in connection with' requirement is satisfied. That requirement is met in a case where, as here, the misappropriated information is a magazine column that has a known effect on the prices of the securities of the companies it discusses.").
[39] United States v. Bonthu, 1:18-CR-237, 2018 WL 3407781 (N.D. Ga. June 28, 2018).
[40] Ken Kam, *After Falling 33%, Equifax Is Still Overvalued*, FORBES (Sept. 21, 2017), https://www.forbes.com/sites/kenkam/2017/09/21/after-falling-33-equifax-is-still-overvalued/#7826c8212b88

insider trading could be problematic because the hackers did not profit from the use of non-public material information usually at issue in insider trading prosecutions (e.g., earnings reports or knowledge of an upcoming acquisition). Rather, our hypothetical hackers would be trading on the basis of their prediction that their cyberattack would drive down the company's stock price.

II. RECONCEPTUALIZING INSIDER TRADING FROM THE OUTSIDE: THE SEC'S AFFIRMATIVE MISREPRESENTATION THEORY

The inability of the classical and misappropriation theories to hold hackers liable does not necessarily render Section 10(b) irrelevant. The Supreme Court has never expressly narrowed the meaning of "deceptive" as it is used in Section 10(b) to trading on the basis on information used in breach of a fiduciary duty.[41] While the theory of fraud in classical and misappropriation cases is based on the defendant's failure to disclose their intent to trade on confidential information, Section 10(b) is not expressly limited to "fraud through silence."[42] This statutory interpretation provided the SEC with the breathing room to develop a new theory of liability aimed at bringing hackers within the ambit of Section 10(b). The SEC's outsider trading theory dispenses with a breach of duty requirement by treating the defendant's hacking and trading as an affirmative material misrepresentation.[43]

A. *SEC v. Dorozhko*: Applying Section 10(b) to hacker-traders.

The SEC relied on the affirmative misrepresentation theory when it brought its first enforcement action against a hacker-trader in 2005.[44] In *SEC v. Lohmus Haavel & Viisemann*, an Estonian investment bank and two of its employees allegedly traded securities after obtaining 360 confidential soon-to-be-released press releases of U.S. companies through the use of a clandestine "spider" program, which scoured information in a business newswire's website.[45] However, the SEC's new theory went untested in *Viisemann* due to the defendants reaching a

(reporting a 33% decline in Equifax stock price, falling from $143 to $96, since the news broke on September 7 that it had been hacked).

[41] "Conduct itself can be deceptive . . . ." Stoneridge Inv. Partners, LLC v. Sci.-Atlanta, 552 U.S. 148, 158 (2008). The dissent in *Stoneridge* noted that the majority "correctly explain[ed] why [Section 10(b)] covers nonverbal as well as verbal deceptive conduct." *Stoneridge*, 552 U.S. at 168 (Stevens, J., dissenting).

[42] "[F]raud through silence is not the only theory of liability actionable under Section 10(b) . . . ." Brian A. Karol, Note, *Deception Absent Duty: Computer Hackers & Section 10(B) Liability*, 19 U. MIAMI BUS. L. REV. 185, 205 (2011).

[43] *Id.* at 211-12.

[44] Stark, *supra* note 25.

[45] Complaint at 7, SEC v. Lohmus Haavel & Viisemann, No. 05-CV-9259 (S.D.N.Y. May 30, 2007). A "spider" program visits websites and collects information. Stark, *supra* note 25.

settlement.[46] A similar scheme was alleged in *SEC v. Blue Bottle Ltd.*, which ended in a settlement as well.[47]

It was not until the 2008 case of *SEC v. Dorozhko* that a court squarely faced the issue of whether to expand insider trading liability to hackers.[48] The defendant in *Dorozhko* was a Ukrainian who hacked into a computer server maintained by Thomson Financial (an investor relations and web-hosting company), providing him access to company earnings reports prior to public release.[49] The hacker purchased put options on the stock after he discovered unreleased negative earnings release of a health company.[50] Upon the release of the negative earnings report, the stock price declined, netting the hacker a profit of $286,456.59.[51]

At issue in *Dorozhko* was whether computer hacking constitutes a "deceptive device" within the meaning of Section 10(b) and Rule 10b-5 where the defendant traded on the basis of material non-public information obtained without the defendant breaching a fiduciary duty.[52] The district court first determined that Section 10(b)'s prohibition on "manipulation" did not apply because the hacker's conduct "did not 'control' or 'artificially affect' market activity, it *was* market activity."[53] This left Section 10(b)'s ban on deception in connection with the purchase or sale of securities as the only grounds of liability.

---

[46] Robert Steinbuch, *Mere Thieves*, 67 Md. L. Rev. 570, 591 n.130 (2008) (noting the settlement required the defendants to disgorge $13 million).

[47] SEC v. Blue Bottle Ltd., No. 07-CV-1380 (CSH) (S.D.N.Y. Feb. 26, 2007).

[48] SEC v. Dorozhko, 606 F. Supp. 2d 321 (S.D.N.Y. 2008), *vacated*, 574 F.3d 42, 43-44 (2d Cir. 2009); Mitts & Talley, *supra* note 13, at 38 ("[I]n *SEC v. Dorozhko*, the SEC had its best (and sole) opportunity thus far to establish a beachhead for outsider trading theory.").

[49] The SEC conceded that "[n]ot all of the details of how Dorozhko accomplished his hack are known." Opening Brief for Appellant at 24, *Dorozhko,* 606 F. Supp. 2d 321. However, the government was able to determine that "spoofing" was one of the techniques Dorozhko employed, a technique that allows a hacker to make their internet traffic appear as if it were originating from a different IP address. *Dorozhko*, 606 F. Supp. 2d at 325 n.3.

[50] According to a report by a cybersecurity firm, many high-profile insider trading cases involve healthcare and pharmaceutical companies, possibly because "stocks in these industries can move dramatically in response to news of clinical trial results, regulatory decisions, or safety and legal issues." BARRY VENGERIK ET AL, HACKING THE STREET? FIN4 LIKELY PLAYING THE MARKET 5, FIREEYE (2014), https://www2.fireeye.com/fin4.html.

[51] *See* Andrew N. Vollmer, *Computer Hacking and Securities Fraud* (Virginia Law & Econ. Research Paper No. 26, 2015), https://ssrn.com/abstract=2679092; Michael D. Wheatley, *Apologia for the Second Circuit's Opinion in* SEC v. Dorozhko, 7 J.L. ECON. & POL'Y 25, 27 (2010).

[52] SEC v. Dorozhko, 606 F. Supp. 2d 321, 324 (S.D.N.Y. 2008), *vacated*, 574 F.3d 42 (2d Cir. 2009). Regarding the other Section 10(b) elements, the district court observed that the scheme was sufficiently "in connection with" the purchase or sale of securities because of the scheme's cohesiveness and the close temporal proximity of the hacking to the trading, noting the hacking and trading occurred within twenty-four hours of each other. *See id.* at 328-29.

[53] *Id.* at 329. The district court explained that the Supreme Court has interpreted "manipulation" to refer to "practices such as wash sales, matched orders, or rigged prices that are intended to mislead investors by artificially affecting market activity." *Id.* (quoting Santa Fe Indus. v. Green, 430 U.S. 462, 476 (1977)).

In order to determine whether the hacking constituted a deceptive device, the district court looked to three Supreme Court cases—*Chiarella v. United States*,[54] *United States v. O'Hagan*,[55] and *SEC v. Zandford*[56]—and concluded that the classical and misappropriation theories both required that the defendant breach a fiduciary duty.[57] Because Dorozhko was an outsider who did not owe a "fiduciary or similar duty either to the source of his information or those he transacted with in the market," the court denied the SEC's request for a preliminary injunction freezing Dorozhko's trading account.[58]

The Second Circuit disagreed. The unanimous three-judge panel first held that a breach of duty was not required in order for "hacking and trading" to be considered a deceptive device.[59] The Second Circuit distinguished the three cases relied upon by the district court, explaining that those decisions all involved a theory of fraud based on silence or nondisclosure of the defendant's intent to use the information to trade securities.[60] The court held that no breach of duty was required where the alleged fraud is based on affirmative misrepresentations.[61]

---

[54] In Chiarella v. United States, the Supreme Court held that "[w]hen an allegation is based upon nondisclosure, there can be no fraud absent a duty to speak," and explained that "a duty to disclose under Section 10(b) does not arise from the mere possession of non-public market information." 445 U.S. 222, 235 (1980) (holding that defendant was not an insider under the classical theory, and was thus wrongly convicted).

[55] *O'Hagan*, 521 U.S. 642 (1997).

[56] *Zandford*, 535 U.S. 813 (2002). In *Zandford*, the defendant securities broker traded under a client's account and transferred the proceeds to his own account. The Fourth Circuit held that the fraud was not "in connection with" the purchase or sale of a security because it was mere theft that happened to involve securities, rather than securities fraud. The Supreme Court reversed, explaining that Section 10(b) "should be construed not technically and restrictively, but flexibly to effectuate its remedial purposes." *Id.* at 819. At the same time however, the Court cautioned against construing the statute "so broadly as to convert every common-law fraud that happens to involve securities into a violation . . . ." *Id.* at 820.

[57] *See Dorozhko*, 606 F. Supp. 2d at 332-38. *See, e.g.,* Regents of the Univ. of Cal. v. Credit Suisse First Boston (USA), Inc., 482 F.3d 372,386 (5th Cir. 2007) ("An act cannot be deceptive within the meaning of §10(b) where the actor has no duty to disclose.").

[58] The district court found it "noteworthy" that in the over seventy years since Congress enacted the Exchange Act, "no federal court has ever held that those who steal material non-public information and then trade on it violate § 10(b) . . . ." *Dorozhko*, 606 F. Supp. 2d at 339. The district court also noted policy considerations that weigh . . . against discarding the fiduciary requirement," explaining that "[w]ithout the fiduciary requirement, the question of when market participants may trade on informational disparities becomes much more difficult." *Id.* at 343.

[59] SEC v. Dorozhko, 574 F.3d 42 (2d Cir. 2009); *See generally* Ryan H. Gilinson, *Clicks and Tricks How Computer Hackers Avoid 10b-5 Liability*, 82 BROOK. L. REV. 1305, 1306–07 (2017) (explaining that the Second Circuit "devised a third theory of liability called the affirmative misrepresentation theory").

[60] *Dorozhko*, 574 F.3d at 48. The court explained that "the SEC has not alleged that the defendant fraudulently remained silent in the face of a 'duty to abstain or disclose' from trading. Rather, the SEC argues that defendant affirmatively misrepresented himself in order to gain access to material nonpublic information, which he then used to trade." *Id.* at 49.

[61] *Dorozhko*, 574 F.3d at 48-49 (reasoning a violation of the "affirmative obligation in commercial dealings not to mislead" is "a distinct species of fraud"); Mitts & Talley, *supra* note 13, at 39.

Having established that a breach of duty was not a necessary condition for a Section 10(b) claim, the court went on to address whether Dorozhko's alleged hacking was deceptive. The court defined "deceptive" according to its ordinary meaning, covering "a wide spectrum of conduct involving cheating or trading in falsehoods" and "irreducibly entails some act that gives the victim a false impression."[62]

The court then described the alleged computer "hacking" as using "electronic means to trick, circumvent, or bypass computer security in order to gain unauthorized access to computer systems, networks, and information . . . and to steal such data."[63] However, the Second Circuit "infused ambiguity into its (otherwise clear) opinion"[64] by including the SEC's "further gloss," which defined "hacking" in general as either (1) "engag[ing] in false identification and masquerade[ing] as another user," or (2) "exploit[ing] a weakness in [an electronic] code within a program to cause the program to malfunction in a way that grants the user greater privileges."[65] According to the Second Circuit, conduct falling under the first category was plainly "deceptive."[66] As to the latter, however, the court felt it was "unclear" whether "exploiting a weakness in an electronic code to gain unauthorized access is 'deceptive,' rather than being mere theft."[67] In other words, determining whether hacking amounts to deception or mere theft "depend[s] on how the hacker gained access" to the information—that is, a fact-intensive and highly technical inquiry.[68]

The Second Circuit remanded the case to the district court so that it could determine whether Dorozhko's hacking amounted to a deceptive device. But this question was ultimately left unanswered.[69] *Dorozhko* remains the sole hacker-trader case adjudicated by a judge.[70] As result, the SEC's affirmative misrepresentation theory, "while partially vetted by the Second Circuit, still remains untested."[71]

---

[62] Mitts & Talley, *supra* note 13, at 39.
[63] *Dorozhko*, 606 F.Supp.2d at 329.
[64] Mitts & Talley, *supra* note 13, at 39.
[65] *Dorozhko*, 574 F.3d at 51.
[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] The district court granted summary judgment to the SEC because defense counsel was unable to establish contact with his client. Stark, *supra* note 25.
[70] Stark, *supra* note 25 (noting "all of the other SEC matters have settled or remain otherwise unresolved").
[71] Stark, *supra* note 25.

B. *SEC v. Dubovoy, et al.*: Extending the affirmative misrepresentation theory to hacker-sellers.

Prior to *Dorozhko*, "no federal court had ever held that the theft of material non-public information by a corporate outsider who subsequently trades securities based on that information violates Section 10(b)."[72] The *Dorozhko* decision sparked a debate over the role of the SEC in computer hacking cases and whether Section 10(b) should apply to a defendant who does not breach a duty to the shareholders or source of information. But it did not take long until another case posed even thornier questions. Whereas *Dorozhko* involved a "hacker-trader" (i.e., a hacker who trades on the confidential information he obtained through a cybersecurity breach), *SEC v. Dubovoy* involved a "new breed of hacker, the so-called hacker-seller," that is, a hacker who obtains insider information and then sells that information to a trader.[73]

In the summer of 2015, the Justice Department filed criminal complaints against several hacker-sellers and their trader accomplices.[74] A few days later, the SEC filed a parallel civil action.[75] At the center of *Dubovoy* was an international scheme involving over 32 defendants. Then-SEC Chair Mary Jo White described the *Dubovoy* case as "unprecedented in terms of the scope of the hacking, the number of traders, the number of securities traded and profits generated."[76] From 2010 until 2014, Ukrainian hackers gained unauthorized access to the computer systems of three business newswires and acquired over 100,000 advance copies of press releases.[77] The hackers then sold the non-public financial information to traders located

---

[72] James A. Jones II, *Outsider Hacking and Insider Trading: The Expansion of Liability Absent a Fiduciary Duty*, 6 WASH. J. L. TECH. & ARTS 111, 116 (2010).
[73] Ryan H. Gilinson, *Clicks and Tricks How Computer Hackers Avoid 10b-5 Liability*, 82 BROOK. L. REV. 1305, 1306 (2017).
[74] Indictment, United States v. Turchynov et al., No. 2:15-cr-00390-MCA, 2015 WL 4764144 (D.N.J. Aug. 6, 2015); Indictment, United States v. Korchevsky, No. 15-cr-381, 2015 WL 4749247 (E.D.N.Y. Aug. 5, 2015).
[75] Complaint, SEC v. Dubovoy et al., No. 15-cv-06076 (D.N.J. Aug. 10, 2015) [hereinafter *Dubovoy Complaint*]. *See, e.g.*, Press Release, U.S. SEC. & EXCH. COMM'N, *SEC Charges 32 Defendants in Scheme to Trade on Hacked News Releases* (Aug. 11, 2015) [hereinafter *Press Release* 2015-163], https://www.sec.gov/news/pressrelease/2015-163.html; Litigation Release No. 23458, U.S. SEC. & EXCH. COMM'N, SEC Obtains $4.2 million from Trader in Hacked News Release Scheme (Feb. 2, 2016), https://www.sec.gov/litigation/litreleases/2016/lr23458.htm (adding two more defendants); Litigation Release No. 23471, U.S. SEC. & EXCH. COMM'N, SEC Charges Nine Additional Defendants in Hacked News Release Scheme (Feb. 18, 2016), https://www.sec.gov/litigation/litreleases/2016/lr23471.htm (adding nine more defendants).
[76] *Press Release* 2015-163, *supra* note 75.
[77] *Dubovoy Complaint, supra* note 75 at 22. Mathew J. Schwartz, *Insider Trading Hack: 5 Takeaways*, BANKINFO SECURITY (Aug. 12, 2015), ("[T]he attackers appeared to employ a mixture of phishing attacks and SQL injection attacks, plus brute-force password guessing, stealing usernames and hashed passwords for offline cracking, as well as installing malware on breached servers to maintain persistent, remote access."), https://www.bankinfosecurity.com/insider-trading-hack-5-takeaways-a-8472.

throughout the world, including Russia, Ukraine, Malta, Cyprus, France, and the United States.[78] These traders in turn purchased or sold "securities depending on their anticipation of how the market would respond to the information in the stolen press releases,"[79] reaping approximately $100 million in illegal profits.[80]

The complaint filed in *Dubovoy* reveals the SEC's conscious effort to frame a theory of liability in accordance with the *Dorozhko* court's concept of hacking. For example, the SEC alleged that the hacker-sellers "used deceptive means to gain unauthorized access" to the news reports, such as "employing stolen username/password information . . . to pose as authorized users . . . [and] concealing the identity and location of the computers used to access the Newswire Services' computers."[81] At the same time, however, the complaint reveals the SEC's attempt to expand the type of hacking tactics that should be deemed "deceptive." For example, the SEC alleged that the hackers deployed "malicious computer code designed to delete evidence of the computer attacks" and used "back-door access-modules."[82] Such techniques do not involve the misrepresentation of one's identity and are more akin to "exploiting a weakness in an electronic code," which *Dorozhko* suggested as amounting to mere theft.[83]

The facts in *Dubovoy* raised another issue. Compared to hacker-trader cases, hacker-seller schemes require a more strained interpretation of Section 10(b)'s requirement that the deceptive device be "in connection with" the purchase or sale of securities.[84] As one commentator describe the problem in hacker-seller schemes, "More than one person's actions were required to create liability under 10b-5: The hackers hacked but did not trade; the traders traded but did not hack."[85] The "in connection with" element was clearly present in *Dorozhko*, where the hacker masqueraded as an authorized user and traded on the stolen information

[78] *Dubovoy Complaint*, *supra* note 75 at 5-6.
[79] *Dubovoy Complaint, supra* note 75 at 6; *see also Press Release* 2018-163, *supra* note 75.
[80] *SEC v. Dubovoy*, No. 15 Civ. 6076, 2016 WL 7217607, slip op. at 1 (D.N.J. Dec. 13, 2016).
[81] *Dubovoy Complaint*, *supra* note 75 at 22.
[82] *Dubovoy Complaint*, *supra* note 75 at 22.
[83] *Dorozhko*, 574 F.3d at 51; *see also* Robert A. Horowitz & Geoffrey S. Berman, *Computer Hacking and Insider Trading Liability*, 31 No. 9 WESTLAW J. CORP. OFFICERS & DIRECTORS LIABILITY 2 (Nov. 2, 2015).
[84] SEC v. Zandford, 535 U.S. 813, 822 (2002) (holding that "in connection with" means "to coincide").
[85] Ryan H. Gilinson, *Clicks and Tricks How Computer Hackers Avoid 10b-5 Liability*, 82 BROOK. L. REV. 1305, 1325 (2017).

himself within a short time frame. Hacker-seller schemes involve a more attenuated link between the hacking and trading.[86]

It has been suggested that hacker-seller cases essentially involve tipper-tippee liability.[87] In classical and misappropriation cases, a tipper is liable if he breaches a duty of confidentiality, which occurs "when the tipper discloses the inside information for a personal benefit."[88] "The tippee acquires the tipper's duty to disclose or abstain from trading if the tippee knows the information was disclosed in breach of the tipper's duty, and the tippee may commit securities fraud by trading in disregard of that knowledge."[89] As explained above, hacking cases do not fit within the traditional theories of insider trading because they lack any such duties. Thus, it is unclear whether a court would expand tipper liability to encompass hacker-sellers and their accomplice traders.[90]

III. POSSIBLE APPROACHES TO HOLDING HACKERS LIABLE AND THE PROBLEMS POSED BY NOVEL HACKING SCHEMES

A. Arguments against holding hackers liable under Section 10(b).

The district court in *Dorozhko* took the position that while "hacking and trading" schemes should be beyond the purview of securities law, hacker-traders ought to be prosecuted under "any number of federal and/or state criminal statutes" for computer fraud.[91] In support of this view, commentators argue that computer hacking is nothing more than mere theft, comparing hackers to burglars who break into a building in order to steal corporate secrets.[92]

---

[86] For example, "[i]n one particularly dramatic instance on May 1, 2013, the [*Dubovoy*] hackers and traders allegedly moved in the 36-minute period between a newswire's receipt and release of an announcement that a company was revising its earnings and revenue projections downward." *Press Release* 2015-163, *supra* note 75; *see Dubovoy Complaint*, *supra* note 77 at 44.

[87] Horowitz & Berman, *supra* note 83 at 3.

[88] Salman v. United States, 137 S. Ct. 420, 423 (2016).

[89] *Id.*

[90] *See* Ryan H. Gilinson, *Clicks and Tricks How Computer Hackers Avoid 10b-5 Liability*, 82 BROOK. L. REV. 1305, 1332 (2017) (arguing that an "aiding and abetting theory is better suited for charging hacker-sellers with insider trading than 10b-5 . . . .").

[91] *Dorozhko*, 606 F. Supp. 2d at 323.

[92] *See* Steven M. Bainbridge, *Ruling on Hackers as Inside Traders: Right in Theory, Wrong on the Law*, LEGAL BACKGROUNDER (Oct. 9, 2009), www.wlf.org/Upload/legalstudies/legalbackgrounder/100909Bainbridge_LB.pdf ("Calling computer hacking a lie is a rather considerable stretch. At most, the hacker 'lies' to a computer network, not a person. Hacking is theft; not fraud."). Critics have disputed the theft analogy by arguing that "the actus reus of theft requires a taking and removing of the property at issue. When the property is virtual information, a hacker may gain access to it and use it without ever having physically removed the information from the computer." Hagar Cohen, *Cracking Hacking: Expanding Insider Trading Liability in the Digital Age*, 17 SW. J. INT'L L. 259, 269 (2011). "The second issue is that of the mens rea of the hacker. Under the traditional theft definition, the thief must

Such conduct is not deceptive and thus, not securities fraud. Critics, such as Andrew Vollmer, contend that the SEC's affirmative misrepresentation theory demonstrates the "dangers of over-zealous pursuit of securities law violations."[93] The government should apply existing laws or enact a new statute to hold hackers liable, rather than "using untested and broadened legal theories [which] creates uncertainty and unpredictability about the scope of securities fraud."[94]

Rather than relying on Section 10(b), the task of prosecuting hackers should instead be left to the DOJ, who can bring charges for computer fraud under the Computer Fraud and Abuse Act (CFAA). It has been argued that the CFAA does not suffer from the same flaws as securities law. For example, the CFAA would apply liability to hacker-sellers in situations where there is a lack of sufficient coordination between the hacker and the traders (thus, not satisfying Section 10(b)'s "in connection with" requirement").[95] Such an approach would also allow the SEC to use its finite resources more effectively.[96]

B. Arguments in favor of holding hackers liable under Section 10(b).

Opposing this view are a majority of commentators who concede that the classical and misappropriation theories of insider trading liability do not cover hacker-traders, but nevertheless believe Section 10(b) should apply.[97] For example, Elizabeth Odian argues that while *Dorozhko*'s "theory of insider trading liability does not comport with current securities law, history and good policy favors a finding that computer hacking is in fact deceptive under Section 10(b) . . . ."[98] She notes that applying Section 10(b) to hacking is in line with the statute's

---

have the intent 'of depriving the true owner of [the personal property].'" *Id.* at 270. But in most hacking situations, the hacker's goal is accessing another's information, not depriving them of the information. *Id.*

[93] Andrew N. Vollmer, *Computer Hacking and Securities Fraud* (Virginia Law & Econ. Research Paper No. 26, 2015), https://ssrn.com/abstract=2679092.

[94] *Id.*

[95] Mitts & Talley, *supra* note 13, at 44.

[96] According to Jaclyn Collier, "[t]he SEC expended considerable resources to pursue the hacker Defendants in *Dubovoy* based on relatively rarefied case law." Jaclyn Collier, *From the Outside In: A Law and Economics Perspective on Insider Trading Cases Involving Cybercrime*, 17 J. HIGH TECH. L. 141, 147 (2016) (noting that at least nineteen SEC employees worked on *Dubovoy*).

[97] DONALD C. LANGEVOORT, 18 INSIDER TRADING: REGULATION, ENFORCEMENT & PREVENTION § 6:14 (noting that *Dorozhko* poses the question of whether a new approach to insider trading ought to be recognized but opining that profiting from stolen information "plainly threatens market integrity"); Donna M. Nagy, *Reframing the Misappropriation Theory of Insider Trading Liability: A Post*-O'Hagan *Suggestion*, 59 OHIO ST. L.J. 1223, 1249-57 (1998) (doubting that a hacker-trader would violate Section 10(b)); Robert A. Prentice, *The Internet and Its Challenges for the Future of Insider Trading Regulation*, 12 HARV. J.L. & TECH. 263, 296-98 (1999) (noting that "from a traditional point of view" hacking and trading is not covered under insider trading theories, but advancing policy considerations for why hackers should be held liable).

[98] Elizabeth A. Odian, *SEC v. Dorozhko's Affirmative Misrepresentation Theory of Insider Trading: An Improper Means to a Proper End*, 94 MARQ. L. REV. 1313, 1339 (2011).

original intent, which was "designed to encompass the infinite variety of devices by which undue advantage may be taken of investors and others."[99] In addition, Odian argues that computer hacking violates Section 10(b) on the "integrity of the market rationale," explaining that one goal of Section 10(b) 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."[100] Thus, prohibiting conduct that threatens market integrity, such as insider trading and hacking, "would increase investor confidence that they are not trading at an informational disadvantage."[101]

In response to the proposal that the DOJ exercise sole oversight of hacking cases, proponents counter that "[c]riminal penalties for computer fraud are insufficient where the misappropriated information is used to trade in securities."[102] They reason that the SEC, unlike the DOJ, "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."[103] Furthermore, it has been suggested that the DOJ and SEC often cooperate in complex investigations, and thus, it would be difficult for the DOJ to pursue CFAA claims against hacker-traders without the SEC's regulatory expertise.[104]

But even among those who support holding hackers liable for insider trading, there are differences of opinion over the exact theory of liability. Some, such as Elizabeth A. Odian support the "fraud on the investors" theory, which Chief Justice Burger promoted in his dissenting opinion in *Chiarella*.[105] They both argue that "insider trading liability [should apply] to insiders and outsiders *whenever* the party transacting on the basis of the inside information obtaines an informational advantage in a manner that public investors may not lawfully overcome."[106] A more expansive approach is the parity of information theory, which "would

---

[99] *Id.* (quoting *In re Cady, Roberts & Co.*, 40 S.E.C. 907, 911 (1961)).
[100] *Id.* at 1341.
[101] *Id.*
[102] *Id.* at 1343.
[103] *Id.*; *see* Brian A. Karol, *Deception Absent Duty: Computer Hackers & Section 10(B) Liability*, 19 U. MIAMI BUS. L. REV. 185, 215 (2011) ("Computer hackers should still remain liable under the CFAA, as well as the mail and wire fraud statutes, but the availability of these provisions should not hinder the authority given to the SEC by Congress in Section 10(b).").
[104] Mitts & Talley, *supra* note 13, at 45.
[105] Chiarella v. United States, 445 U.S. 222, 240 (1980) (Burger, C.J., dissenting).
[106] Hagar Cohen, *Cracking Hacking: Expanding Insider Trading Liability in the Digital Age*, 17 SW. J. INT'L L. 259, 273 (2011); Elizabeth A. Odian, *supra* note 98, at 1347-48.

prohibit trading on all non-public material regardless of the manner in which the investor gained access to such information."[107] The *Chiarella* Court explicitly rejected the parity of information theory, but left open the possibility for the fraud on the investor approach.[108]

C. Modifying the misrepresentation theory in order to address deceptive hacking schemes that do not involve the theft of insider information.

Normatively, the Second Circuit's endorsement of the affirmative misrepresentation theory in *Dorozhko* was a step in the right direction, but the decision also raises potential problems. On the one hand, the court's focus on whether the defendant's hacking techniques were deceptive is supported by the plain language of Section 10(b). Arguably, there is more textual support for the affirmative misrepresentation approach than the misappropriation theory, which has been criticized as being based more on a nondeceptive state law breach of fiduciary duty.[109]

On the other hand, the Second Circuit's definition of "hacking" failed to provide clear guidance for future cases and potentially shields future hackers from liability. First, the court's description of Dorozhko's hacking as "employ[ing] electronic means to trick, circumvent, or bypass computer security in order to gain unauthorized access to computer systems, networks, and information . . . and to steal such data," suggests a general definition of "hacking" that is limited to conduct that obtains confidential information.[110] Second, the court further limited this definition when it explained that hacking comprises of two techniques: either masquerading as other users or exploiting software vulnerabilities.[111] While masquerading one's identity is a straightforward example of deceptive conduct, the court seems to suggest that it is the only deceptive hacking technique, thus, leaving open the possibility of innovative hackers to avoid liability in future cases.

The Second Circuit's approach illustrates the problems with attempts to pigeonhole hackers within the typical insider trading framework. Current insider trading law equates a

---

[107] Elizabeth A. Odian, *supra* note 98, at 1345. The parity of information theory has been rejected by the Supreme Court as being overly broad. *See* Dirks v. SEC, 463 U.S. 646, 658-59 (1983).
[108] "[I]t is my understanding that the Court has not rejected the view, advanced above, that an absolute duty to disclose or refrain arises from the very act of misappropriating nonpublic information." *Chiarella*, 445 U.S. at 243 n. 4 (Burger, C.J., dissenting).
[109] Robert A. Prentice, *The Internet and Its Challenges for the Future of Insider Trading Regulation*, 12 HARV. J. L. & TECH. 263, 297 (1999).
[110] SEC v. Dorozhko, 574 F.3d 42, 50 (2d Cir. 2009).
[111] *Id.* at 51.

breach of fiduciary duty with the fraud requirement.[112] It is not the possession of confidential information that gives rise to a claim, but rather using the information in a manner that breaches the duty. But fiduciary duties could theoretically be breached in ways that do not involve the unauthorized use of confidential information. By way of extreme example, it would arguably be just as deceptive if a corporate insider feigned loyalty to the company, but secretly sabotaged the company's operations in order to drive down the stock value and reap the profits from put options. In such a situation, the defendant would be committing deception by feigning loyalty but secretly causing damage to the company—not his use of confidential information to his advantage.

Similarly, Section 10(b) should not be limited to deceptive hacking techniques that give the hacker access to insider information. *Dorozhko*'s view of hacking as conduct that steals information has the potential to exclude deceptive cyberattacks (e.g, hiding one's identity) in connection with securities trading, but do not result in the attackers gaining confidential information. For example, hackers could buy put options on companies, target the companies with distributed denial-of-service ("DDoS") attacks[113] or ransomware attacks,[114] and then release news of the attacks causing a decline in stock price. These cyberattacks could be considered deceptive within the meaning of *Dorozhko* but would unlikely result in liability because they do not provide the hackers with inside information.[115]

---

[112] United Stated v. O'Hagan, 521 U.S. 642, 652-53 (1997).

[113] DDoS attacks are defined as rendering an online service unavailable though the use of multiple sources sending a flood of overwhelming traffic. White House Council of Economic Advisers, *The Cost of Malicious Cyber Activity to the U.S. Economy,* THE WHITE HOUSE 2 (Feb. 16, 2018), https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf. DDoS attacks require the attacker to infect numerous computers and other machines with malware, turning each one into a "bot." The attacker then directs the bots to send a flood of requests to the victim's Internet Protocol ("IP") address. *What is a DDoS Attack?*, CLOUDFLARE, https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ (last visited Apr. 7, 2018).

[114] "Ransomware is a type of malware that infects a computer and restricts a user's access to the infected computer." US-CERT, *Crypto Ransomware*, NCCIC (Sept. 30, 2016), https://www.us-cert.gov/ncas/alerts/TA14-295A. "Ransomware is typically spread through phishing emails that contain malicious attachments and drive-by downloading. Drive-by downloading occurs when a user unknowingly visits an infected website and malware is downloaded and installed without their knowledge. Crypto ransomware, a variant that encrypts files, is typically spread through similar methods . . . ." *Id.* In other words, ransomware is not intended to gain access to the contents of the information, but the attack is arguably "deceptive" if it is spread via phishing.

[115] As noted above, ransomware attacks would usually constitute a deceptive device under Section 10(b) because ransomware usually relies on phishing and social engineering in order to trick the user to run a malicious program. However, not all ransomware relies on deceptive techniques and thus, would arguably fall outside Section 10(b). For example, in March 2018, the city of Atlanta, Georgia was the victim of a costly ransomware attack. The attackers used the SamSam ransomware, which utilizes a brute-force attack to guess weak passwords, rather than phishing.

Indeed, the market continues to react to news of cyberattacks more quickly as investors continue to gain a better understanding of the costs of cyberattacks.[116] A study of 65 companies affected by hacking incidents since 2013 concluded that cyberattacks have a debilitating effect on stock prices, "causing an average decline of 1.8% on a permanent basis in cases of severe breaches."[117] And another study concluded that among the various forms of cyberattacks, "DDoS attacks are a distant second in terms of the damage caused, with the attacked firms losing 2.41 percent of market value…"[118]

In short, Section 10(b) liability should not be limited to hackers that obtain insider information. Rather, courts should simply ask whether the defendant's hacking amounted to a "deceptive device" in connection with the purchase or sale of securities. A plain reading of Section 10(b) does not require the theft of confidential insider information in order for there to be deception.[119] Such an approach is essentially an expansion of the SEC's affirmative misrepresentation theory and Donna Nagy's "deceptive acquisition theory."[120]

Under this approach, a court would first determine whether the defendant engaged in hacking, which would be given a broad definition—possibly one based on the National Research Council's concept of "cyberattack."[121] This would generally include the following activities: (1)

See Lily Hay Newman, *The Ransomware That Hobbled Atlanta Will Strike Again*, WIRED (Mar. 30, 2018), https://www.wired.com/story/atlanta-ransomware-samsam-will-strike-again/.

[116] White House Council of Economic Advisers, *The Cost of Malicious Cyber Activity to the U.S. Economy,* THE WHITE HOUSE 9 (Feb. 16, 2018), https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

[117] Matthew Heller, *Cyber Attacks Can Cause Major Stock Drops*, CFO (Apr.12, 2017), http://ww2.cfo.com/cyber-security-technology/2017/04/cyber-attacks-stock-drops/.

[118] White House Council of Economic Advisers, *The Cost of Malicious Cyber Activity to the U.S. Economy*, THE WHITE HOUSE 12 (Feb. 16, 2018), https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

[119] The focus should be on deception, insider trading is merely one form of deception. *See* Webster's International Dictionary 679 (2d ed. 1934) (defining "deceptive" as "tending to deceive," and defining "deceive" as "[t]o cause to believe the false, or to disbelieve the true" or "[t]o impose upon; to deal treacherously with; cheat"); *Cf.* Ernst & Ernst v. Hochfelder, 425 U.S. 185, 199 n.20 (1976) (consulting the 1934 edition of Webster's International Dictionary to define other relevant terms in Section 10(b)).

[120] In Donna M. Nagy, *Insider Trading and the Gradual Demise of Fiduciary Principles*, 94 IOWA L. REV. 1315, 1359 (2009), Nagy proposes a theory of deceptive acquisition, which would support "liability in any case where confidential information was acquired through deceptive means, even in the absence of a fiduciary-like relationship between the trader and the source." *Id.* However, this paper proposes a theory that extends beyond Nagy's—which is limited to "scenarios in which a person *obtains confidential information* through lies or other means of trickery"—and would extend liability to hackers that do not deceptively obtain insider information, but nevertheless employ deceptive schemes in connection with securities transactions. *Id.* at 1371 (emphasis added).

[121] According to a report by the National Science Council, "Cyberattack refers to deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks." NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 1 (William A. Owens et al. eds., 2009);

attempts to gain unauthorized access to a system or its data; (2) DDoS attacks; and (3) unauthorized changes to system hardware, firmware, or software.[122]

The court would then determine whether the hacking was "deceptive." *Dorozhko*'s definition of deceptive hacking is instructive—that is, the use of false identification and masquerading as another user. The best example of such deceptive conduct would be phishing,[123] but other tactics, such as using stolen credentials, would fall within the definition of deceptive hacking.[124] Finally, the deceptive conduct would have to be in connection with the purchase or sale of securities.

By way of illustration, this approach would extend liability to defendants who conduct a DDoS attack that temporarily shuts down a corporation's website and in turn, causes an adverse market reaction.[125] Such conduct would arguably be deceptive because during a DDoS attack, each "bot [that is, a computer under the attacker's control] is a legitimate Internet device"—in other words, the attacker uses unwitting computers in order to masquerade as other Internet users in order to flood a victim's website, thereby causing it to crash.[126]

In addition, this approach would likely cover unorthodox ransomware attacks in which the attackers do not seek to profit from the ransom payment itself, but rather use the ransomware to disrupt a company's operations and in turn a temporary decline in the victim's stock. Such a

---

see Matthew F. Ferraro, *Groundbreaking or Broken; An Analysis of SEC Cybersecurity Disclosure Guidance, Its Effectiveness, and Implications*, 77 ALB. L. REV. 297, 307 (2014).

[122] White House Council of Economic Advisers, *The Cost of Malicious Cyber Activity to the U.S. Economy*, THE WHITE HOUSE 2 (Feb. 16, 2018), https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

[123] The United States Computer Emergency Readiness Team (US-CERT) defines "phishing" as "an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques. Phishing emails are crafted to appear as if they have been sent from a legitimate organization or known individual." US-CERT, *Report Phishing Sites*, CISA https://www.us-cert.gov/report-phishing, (last visited Apr. 24, 2018).

[124] For example, in 2016, Chinese hackers made over $4 million from trading on M&A information they stole from Cravath, Swaine & Moore and Weil Gotshal & Manges. *See* Sara Randazzo & Dave Michaels, *U.S. Charges Three Chinese Traders with Hacking Law Firms*, WALL ST. J. (Dec. 27, 2016). The SEC alleged that the hackers used stolen credentials to pose as IT employees and installed disguised malware on the law firms' servers in order to obtain lawyers' emails. Complaint at 11, SEC v. Hong, et al., 16-cv-09947 (S.D.N.Y. Dec. 27, 2016).

[125] One recent study concluded "that there is a noticeable negative impact on the stock prices of the victim firm whenever the attack causes interruptions to the services provided by the firm to its customers." However, the researchers noted that it was "not possible to comment on the intensity of the impact because it is firm dependent." Abhishta, Reinoud Joosten,& L. J. M. Nieuwenhuis, *Analysing the Impact of a DDoS Attack Announcement on Victim Stock Prices*, *2017 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP)* (Mar. 2017).

[126] *What is a DDoS Attack?*, CLOUDFLARE, https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ (last visited April 7, 2018).

scheme would likely be deceptive because ransomware is almost always delivered via phishing e-mails.

In light of the fact that hackers are constantly tweaking their methods, the approach proposed above would likely prove to be more robust than the one followed in *Dorozhko*.[127] Enacting new legislation would be preferable. But in the absence of congressional action, the courts should aim to "interpret Section 10(b) and Rule 10b-5 to meet new challenges in maintaining the integrity of the securities markets."[128] Indeed, the Supreme Court explained decades ago that Section 10(b) "prohibit[s] all fraudulent schemes in connection with the purchase or sale of securities, whether the artifices employed involve a garden type variety of fraud, or present a unique form of deception."[129]

Moreover, an approach such as the one above, which focuses on deception, rather than the theft of insider information, is arguably supported by the actual language of Section 10(b) and precedent interpreting the statute. In *SEC v. Zanford* the Court explained that *O'Hagan* stood for the proposition that in misappropriation cases, a "fiduciary's fraud is consummated, *not when the fiduciary gains the confidential information*, but when, without disclosure to his principal, he uses the information to purchase or sell securities."[130] In other words, Section 10(b) treats the breach of a duty of confidentiality as fraud. Misusing insider information is one way to commit fraud, but the Court has never said that is it the only way. Likewise, trading on insider information obtained through deceptive hacking should constitute actionable fraud, but it should not be the only way. What matters is the deception.

If the SEC is unable to convince a court that a novel cyberattack, such as a ransomware or DDoS attack, amounts to a deceptive device under Section 10(b), then the SEC may consider arguing that such conduct constitutes unlawful market manipulation. The advantage of such an approach is that courts have already held that there is no duty requirement in market manipulation cases.[131]

---

[127] *E.g.,* In a survey of 150 Canadian IT security decision makers, 55% of participants reported security breaches involving a printer and "[a]lmost all included documents thought to contain sensitive or private information." Mary Ann Yule, *The Way Hackers Will Try to Attack Canadian Businesses In 2017*, FORBES (Sept. 6, 2017), https://www.forbes.com/sites/hp/2017/09/06/the-way-hackers-will-try-to-attack-canadian-businesses-in-2017/#33b1f5cc5780.

[128] Odian, *supra* note 98, at 1349.

[129] Superintendent of Ins. v. Bankers Life & Cas. Co., 404 U.S. 6, 10 n.7 (1971).

[130] SEC v. Zandford, 535 U.S. 813, 824 (2002).

[131] *See* ATSI Comm., Inc. v. Shaar Fund, Ltd., 493 F.3d 87, 99-100 (2d. Cir. 2007) (held that market manipulation violates Rule 10b-5 "regardless of whether there is a fiduciary relationship between transaction participants."); *see*

But it is unlikely that a court would characterize a DDoS attack as market manipulation in light of Supreme Court precedent. The Court has explained that "[m]anipulation" is "virtually a term of art . . . refer[ring] generally to practices such as wash sales, matched orders, or rigged prices that are intended to mislead investors by artificially affecting market activity."[132] And the Second Circuit has explained that a manipulator is one who engages "in market activity aimed at deceiving investors as to how other market participants have valued a security."[133] "The deception arises from the fact that investors are misled to believe 'that prices at which they purchase and sell securities are determined by the natural interplay of supply and demand, not rigged by manipulators.'"[134]

The problem is that investors would not be reacting to inaccurate information in our hypothetical cyberattack, in which the attackers disrupt or embarrass a company, thereby driving down consumer confidence in the stock.[135] Instead, investors would be trading at prices that are based on reactions to accurate information (i.e., the company has a legitimate vulnerability).[136] In other words, the release of accurate information that was obtained as a result of deceptive hacking or criminal conduct does not necessarily amount to manipulation.

Therefore, it is likely that all hacking schemes will have to be prosecuted as deception. Nevertheless, there are shortcomings to this paper's modified affirmative misrepresentation theory. First, it requires a court to distinguish between deceptive and nondeceptive hacking tactics—a potentially "technical distinction that will be uncertain in many cases."[137] Indeed, this is perhaps the strongest argument against this approach. Until the Supreme Court holds that "hacking is inherently deceptive, the facts particular to each individual hack will be vital in determining whether a computer hacker dealt in deception."[138]

---

also United States v. Skelly, 422 F.3d 94, 99 n.4 (2d Cir. 2006) (held that a pump-and-dump scheme violates Section 10(b) and Rule 10b-5, despite the defendants owing no fiduciary duty).

[132] Santa Fe Indus. v. Green, 430 U.S. 462, 476 (1977).

[133] ATSI Commc'ns, Inc. v. Shaar Fund, Ltd., 493 F.3d 87, 100 (2d Cir. 2007).

[134] *Id.*

[135] *Id.* at 101. "[T]he Third Circuit distinguishes manipulative from legal conduct by asking whether the manipulator 'inject[ed] inaccurate information into the marketplace or creat[ed] a false impression of supply and demand for the security . . . for the purpose of artificially depressing or inflating the price of the security.'" (quoting GFL Advantage Fund, Ltd. v. Colkitt, 272 F.3d 189, 207 (3d Cir. 2001)).

[136] Mitts & Talley, *supra* note 13, at 3 ("They would not violate market manipulation proscriptions, which require the introduction of inaccurate information into the market.").

[137] Adam R. Nelson, *Extending Outsider Trading Liability to Thieves*, 80 FORDHAM L. REV. 2157, 2194 (2012).

[138] Brian A. Karol, *Deception Absent Duty: Computer Hackers & Section 10(B) Liability*, 19 U. MIAMI BUS. L. REV. 185, 214 (2011).

Second, "it leaves untouchable those investors who obtain non-public information through outright theft, because theft lacks the requisite deception."[139] In the context of hacking, this means that nondeceptive hacking that leads to the acquisition of confidential information would not constitute deception. For example, a defendant would arguably not be committing deception by using SQL injection attacks in order to obtain information from a corporation's database. The reason that thieves would escape liability is not so much a result of the affirmative representation theory but rather the actual language of Section 10(b)—which only applies to "deceptive" or "manipulative" devices.

In short, until a new statute is enacted, there will always remain the potential for hackers to avoid liability through the use of nondeceptive schemes, which may smack of unfairness, but are nevertheless not securities fraud. These innovative tactics would be the flip-side of the traditional pump-and-dump ploy, which uses false information to cause market reactions. The hypothetical hacker would instead use nondeceptive tactics in order to obtain and release accurate information and cause adverse market reactions. Such a scenario is not so farfetched when one considers the phenomenon of "informed cyber-trading," which has been defined as "trading on the basis of advanced knowledge of cybersecurity breach."[140]

In a recent paper, Joshua Mitts and Eric L. Talley observe that "arbitrageurs can and do obtain early notice of impending [cybersecurity] breach disclosures, and . . . profit from such information."[141] Mitts and Talley point to an incident in 2016 involving MedSec, a start-up cybersecurity firm, as an example of informed cyber-trading. MedSec discovered a serious security software flaw in the cardiac pacemakers produced by St. Jude Medical. MedSec informed the short hedge fund Muddy Waters Capital, who then took a short position in St. Jude Medical. Muddy Waters then publicly disclosed news of the vulnerability, which in turn caused St. Jude's stock price to fall in excess of eight percent.[142] As explained below, the Muddy Waters incident demonstrates how hackers could use innovative attacks to avoid liability for securities fraud. In addition, the Muddy Waters case raises interesting policy questions. In particular, it

---

[139] Elizabeth A. Odian, *supra* note 98, at 1346. (Odian argues that 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." *Id.* However, it is unclear whether this is a serious limitation. Would the hacker have to not only disclose his or her intent to trade, but also the hacker's identity? Nevertheless, it is hard to imagine either scenario becoming a reality.)

[140] Mitts & Talley, *supra* note 13, at 2.

[141] *Id*.

[142] *Id*.

could be argued that certain hacking is socially beneficial when it forces companies to address problems it would otherwise refuse to fix, such as manufacturers of vulnerable medical devices[143] or telecommunications companies that fail to adequately safeguard consumer privacy.[144]

Informed-cyber trading demonstrates how nondeceptive tactics lie beyond the scope of Section 10(b). Our hypothetical hacker could infiltrate a company's network or perhaps reverse engineer its product by relying on nondeceptive techniques, which merely "exploit a weakness in code"[145]—such as buffer overflows,[146] Structured Query Language (SQL) injections,[147] or perhaps a zero-day exploit.[148] If the attack successfully breaches the company's defenses, the hacker learns that the company's network, its products, or perhaps its customer data, are vulnerable to theft.[149] Rather than steal confidential information, the hacker would merely sell

---

[143] In 2011 for example, Barnaby Jack, a security researcher, demonstrated the wireless hacking of insulin pumps, causing the pumps to dispense all of the insulin—which would be a surreptitiously delivered fatal dose for a diabetic patient. Dan Goodin, *Insulin pump hack delivers fatal dosage over the air*, THE REGISTER (Oct. 27, 2011), https://www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack/.

[144] Kim Zetter, *Appeals Court Overturn Conviction of AT&T Hacker 'Weev*,' WIRED (Apr. 11, 2014), https://www.wired.com/2014/04/att-hacker-conviction-vacated/ (reporting on the Third Circuit's reversal of a hacker's CFAA conviction in United States v. Auernheimer on venue grounds, but expressing skepticism of the original conviction, noting that the defendant exposed a flaw in AT&T security which allowed iPad users' e-mail addresses to be revealed only through accessing publicly available information and not circumventing any passwords).

[145] SEC v. Dorozhko, 574 F.3d 42, 51 (2d Cir. 2008).

[146] CLOUDFARE, *Buffer Overflow*, https://www.cloudflare.com/learning/security/threats/buffer-overflow/, (last visited Apr. 24, 2018) ("Buffer overflow is an anomaly that occurs when software writing data to a buffer overflows the buffer's capacity, resulting in adjacent memory locations being overwritten. In other words, too much information is being passed into a container that does not have enough space, and that information ends up replacing data in adjacent containers.").

[147] Loren F. Selznick & Carolyn LaMacchia, *Cybersecurity: Should the SEC be Sticking its Nose Under this Tent?*, 2016 U. ILL. J.L. TECH. & POL'Y 35, 62 (2016) ("SQL injection attacks involve sending modified SQL statements to a Web application that, in turn, modifies a database. Attackers send unexpected input through their Web browsers that enable them to read from, write to, and even delete entire databases."); Ryan H. Gilinson describes SQL injection attacks as an example of "structural hacking," which he defines as conduct exploiting "structural deficiencies in the computer to obtain valuable information." Ryan H. Gilinson, *Clicks and Tricks: How Computer Hackers Avoid 10b-5 Liability*, 82 BROOK. L. REV. 1305, 1324 (2017) (distinguishing between "misrepresentative hacking" and "structural hacking").

[148] FIREEYE, *What is a Zero-Day Exploit?*, https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html, (last visited April 23, 2018) ("A zero-day vulnerability, at its core, is a flaw."); Roger Park, *Guide to Zero-Day Exploits*, SYMANTEC OFFICIAL BLOG (Nov. 9, 2015), https://www.symantec.com/connect/blogs/guide-zero-day-exploits ("A zero-day exploit is an undisclosed application vulnerability that could be exploited to negatively affect the hardware, applications, data or network. The term 'zero day' refers to the fact that the developers have 'zero days' to fix a problem that has just been exposed and may have been already exploited.").

[149] It could be argued that a nondeceptive cyberattack that reveals a vulnerability is synonymous with obtaining material non-public information in that the hacker learns that the company's network has an undisclosed vulnerability. However, such information is different than the information in the typical insider trading case because the company is unaware of the information (that is, the company often does not know about the security flaw). In traditional insider trading cases, the defendant obtains information that is already known by the corporation.

knowledge of the vulnerability to traders. The traders would then take a short position in the company and release news of the vulnerability and profit on the resulting decline in stock value.

While the hacker may be liable under the Computer Fraud and Abuse Act (CFAA), he would more than likely avoid Section 10(b) liability. Ironically, the misappropriation theory would hold an outsider liable for trading on the same information if one of the company's IT employees had been aware of the vulnerability and disclosed the information in confidence to the outsider.

Admittedly, applying an eighty-four-year old statute to computer hackers requires fashioning a theory of liability, which if not clearly defined, risks "taking over 'the whole corporate universe.'"[150] A preferable alternative to the affirmative misrepresentation theory would be new legislation.[151] The European Union's insider trading law could serve as a starting point.[152] The E.U.'s regulations essentially take the parity of information approach: "an individual is prohibited from trading on the basis of insider information regardless of how that information was obtained."[153] Specifically, E.U. law prohibits "insider dealing," which "arises where a person possesses inside information[154] and uses that information by acquiring or disposing of, for its own account or for the account of a third party, directly or indirectly, financial instruments to which that information relates."[155] The SEC originally advanced this theory in *In re Cady, Roberts & Co.*, 40 SEC 907 (1961), and *SEC v. Tex. Gulf Sulphur Co.*, 401

---

[150] United States v. Chestman, 947 F.2d 551, 567 (2d Cir. 1991).
[151] Robert Steinbuch, *Mere Thieves*, 67 Md. L. Rev. 570, 611 (2008).
[152] *See* Robert T. Denny, *Beyond Mere Theft: Why Computer Hackers Trading on Wrongfully Acquired Information Should Be Held Accountable under the Securities Exchange Act*, 2010 UTAH L. REV. 963, 979 (2010) ("[C]ongress should enact legislation that prohibits trading on all wrongfully obtained material nonpublic information, regardless of how that information is obtained."); *see also* Hagar Cohen, *Cracking Hacking: Expanding Insider Trading Liability in the Digital Age*, 17 SW. J. INT'L L. 259, 272 (2011) ("The U.S. should follow in the E.U.'s steps in extending liability to *any person* that transacts on the basis of an informational advantage that public investors may not lawfully overcome, regardless of their diligence or resources.").
[153] Hagar Cohen, *Cracking Hacking: Expanding Insider Trading Liability in the Digital Age*, 17 SW. J. INT'L L. 259, 271 (2011) (discussing E.U. Market Abuse Directive (2003/6/EC) ("MAD")). On July 3, 2016, the E.U. adopted a new "Market Abuse Regulation" (596/2014/EU) ("MAR"). The substantive rules under MAR largely mirror the pre-existing rules under MAD. John F. Savarese, Wayne M. Carlin, & Jonathan Siegel, *The New European Union Market Abuse Regulation*, WACHTELL, LIPTON, ROSEN & KATZ (May 3, 2016), https://www.law.ox.ac.uk/business-law-blog/blog/2016/05/new-european-union-market-abuse-regulation.
[154] MAR defines "inside information" as "information of a precise nature, which has not been made public, relating, directly or indirectly, to one or more issuers or to one or more financial instruments, and which, if it were made public, would be likely to have a significant effect on the prices of those financial instruments or on the price of related derivative financial instruments." Commission Regulation 596/2014, art. 7, ¶ 1(a), 57 O.J. (L 173) (EC), available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_. 2014.173.01.0001.01.ENG.
[155] Commission Regulation 596/2014, art. 8, ¶ 1, 57 O.J. (L 173) (EC), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_. 2014.173.01.0001.01.ENG.

F.2d 833 (2d Cir. 1968).[156] In the event that Congress fails to act, then the SEC could consider implementing narrow regulations specifically aimed at hackers.[157]

CONCLUSION

The recent hacking and trading cases highlight the limitations of current insider trading jurisprudence. The classical and misappropriation theories fail to capture hackers because they are corporate outsiders who do not owe fiduciary duties to shareholders and lack any confidential relationship with the source of information. While the Second Circuit's endorsement of the SEC's affirmative misrepresentation theory will help close the gap, the theory is largely limited to hacker-traders that use phishing techniques in order to obtain inside information for trading purposes.

Hackers are by their very definition creative.[158] Thus, it is only a matter of time before they cook up novel cyber-trading schemes that do not involve the theft of inside information and therefore avoid liability, yet are nonetheless deceptive insofar as the hacker misrepresents his or her identity in connection with the purchase or sale of securities.

This paper has offered a modified approach to the SEC's affirmative misrepresentation theory in order to address *Dorozhko*'s shortcoming. Rather than seek to shoehorn hackers within the traditional concept of insider trading and limit liability to hackers that steal confidential information, courts should simply determine whether a hacker employed "manipulative or deceptive" techniques in connection with the purchase or sale of securities. Thus, liability would apply whenever a hacker employs a cyberattack (in which the hacker misrepresents his or her identity) in connection with a securities transaction, regardless of whether confidential information was stolen. Still, it is clear that Section 10(b) cannot cover every potential securities related cyberattack, such as nondeceptive informed cyber-trading. Whether the government should even seek to regulate such conduct is an even harder question.

---

[156] Peter J. Henning, *What's So Bad About Insider Trading Law?*, 70 BUS. LAW. 751, 773 (2015) ("This approach has been enshrined in Rule 14e-3106 for trading on information related to a tender offer, which was endorsed by the Supreme Court in *O'Hagan* as a permissible use of the SEC's rulemaking authority.").

[157] One possible rule would state that Section 10(b) is violated whenever a defendant violates the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, in connection with a securities transaction. *See* Robert T. Denny, *Beyond Mere Theft: Why Computer Hackers Trading on Wrongfully Acquired Information Should Be Held Accountable under the Securities Exchange Act*, 2010 UTAH L. REV. 963, 980 (2010).

[158] Y. ANTO, THE ART OF HACKING 2 (2012) (One definition of "hacker" is "[a] person who uses his creativity and knowledge to overcome limitations, often in technological contexts.").