Brooklyn Law Review

Volume 82 | Issue 3 Article 7

2017

Clicks and Tricks: How Computer Hackers Avoid 10b-5 Liability

Ryan H. Gilinson

Clicks and Tricks

HOW COMPUTER HACKERS AVOID 10b-5 LIABILITY

"You don't need to be a Wall Street insider to pull off insider trading anymore."[1]

INTRODUCTION

Over a five-year period, two hackers residing in the Ukraine hacked into several newswire services that housed press releases containing sensitive financial information. The hacks occurred before the press releases were to be disseminated to the public in order for the hackers to capitalize on the valuable information they contained.[2] Once they acquired the press releases, the hackers distributed them to various traders located in several countries across the world including Russia, Malta, France, the Virgin Islands, and Cyprus.[3] The traders then executed a series of securities transactions on the basis of that information and realized over $100 million in profits.[4] The Securities Exchange Commission (SEC) described this chain of conduct as unprecedented because it had never seen an insider trading case whose conduct lasted that many years, spanned that many countries, and reaped that much profit.[5]

It's not every day that the SEC describes an act of insider trading as "unprecedented."[6] But in many ways that's exactly what the story of the Ukrainian hackers was: a comprehensive insider trading plot orchestrated by a

[1] Klint Finley, *Hackers Busted in Insider Trading Scheme*, WIRED (Aug. 11, 2015), http://www.wired.com/2015/08/hackers-busted-insider-trading-scheme [https://perma.cc/MFA3-JEG].

[2] Complaint for Violations of the Federal Securities Law at 21–23, SEC v. Dubovoy, No. 2:15-cv-06076-MCA-MAH (D.N.J. Aug. 10, 2015) (explaining the financial value of the information the hackers stole).

[3] *Id.* at 2–5 (listing the trader defendants and their locations around the world).

[4] *Id.* at 22–25.

[5] *U.S. Charges 9 with Insider Trading Based on Hacked Press Releases*, NBC NEWS (Aug. 11, 2015), http://www.nbcnews.com/business/business-news/u-s-charges-9-insider-trading-based-hacked-press-releases-n407771 [https://perma.cc/RMA8-SRLH].

[6] *See id.* (quoting SEC chief Mary Jo White) ("Today's international case is unprecedented in terms of the scope of the hacking at issue, the number of traders involved, the number of securities unlawfully traded and the amount of profits generated.").

"sprawling network of hackers and traders"[7] spanning the globe, who unlawfully siphoned over 150,000 news releases from servers belonging to three different U.S. newswire services to facilitate the execution of illegal trades at seemingly impossible speeds,[8] yielding millions of dollars in illegal profits. This story depicted a broader scope of crime, a staggering number of trades, and an immense amount of profits unlike anything the SEC had seen before. While the amount of profits earned by these illicit actions appears the most unsettling, there is another part to the story that is even more striking.

Insider trading is prohibited by Section 10(b) of the 1934 Securities Exchange Act[9] (the Securities Exchange Act) and Rule 10b-5, which criminalizes the use of a manipulative or deceptive device "in connection with the purchase or sale of" securities.[10] Computer hackers have been prosecuted under Section 10(b) and Rule 10b-5 before—when they traded on stolen information themselves[11]—but never when they sold the information they acquired instead. The two Ukrainian hackers represent a new breed of hacker, the so-called hacker-seller. Charging these hackers under 10b-5 becomes complicated because their conduct does not occur "in connection with" a securities transaction; therefore, they seemingly circumvent liability under the securities laws.

There are two primary theories of 10b-5 liability—the classical theory and the misappropriation theory—under which a defendant may be charged with insider trading; these theories complement one another and apply depending on the type of defendant.[12] The Second Circuit recently devised a third theory of liability called the affirmative misrepresentation theory, which attaches liability to affirmative

[7] David Porter, *Group Made $30 Million with Hacked Press Release Info in Insider Trading Scheme: Feds*, NBC 4 N.Y. (Aug. 11, 2015), http://www.nbcnewyork.com/news/local/Hack-Insider-Trading-Securities-Arrest-Millions-Dollars-Computer-System-Indictment-New-Jersey-New-York-321390061.html [https://perma.cc/2UM7-2R2A].

[8] Press Release, SEC, SEC Charges 32 Defendants in Scheme to Trade on Hacked News Releases (Aug. 11, 2015), http://www.sec.gov/news/pressrelease/2015-163.html [https://perma.cc/CM9K-5G59] (explaining that one trade occurred a mere thirty-six minutes between the newswire's receipt and release of an announcement projecting an earnings loss and realizing $511,000 in profits).

[9] Securities Exchange Act of 1934, 15 U.S.C. § 78b (1994).

[10] 17 C.F.R. § 240.10b-5 (2016).

[11] *See, e.g.*, SEC v. Dorozhko, 574 F.3d 42, 43–44 (2d Cir. 2009).

[12] The classical theory pertains to corporate insiders (permanent employees who work for the firm or company in question) and the misappropriation theory pertains to corporate outsiders (non-insiders who "owe[ ] a duty of trust and confidence to someone other than the issuer and its shareholders"). Greg Kramer, *Insider Trading: Examining Primary Theories of Liability*, N.Y.L.J. (Feb. 14, 2013), http://www.newyorklawjournal.com/id=1202588045359/Insider-Trading-Examining-Primary-Theories-of-Liability [https://perma.cc/S9LX-Q7RC].

misrepresentations in connection with the purchase or sale of securities.[13] This theory, unlike the classical or misappropriation theories, does not require a breach of fiduciary duty to the source of the information.[14] Hacker-sellers, however, fall outside all three theories of insider trading liability because they do not owe a fiduciary duty to anyone *and* they do not personally trade on the information they wrongfully acquire.

Section 20(e) of the Exchange Act is the aiding and abetting provision, which enables the SEC to prosecute those who "knowingly or recklessly provide[] substantial assistance to another person" who violates the Act.[15] This provision more appropriately captures the hacker-seller's wrongful conduct than 10b-5 does because it depicts a more accurate characterization of that conduct. 10b-5 prohibits certain conduct related to the "purchase or sale" of securities, but the hacker-seller neither purchases nor sells securities; instead, they sell the information they wrongfully acquire to *another* person, the trader, who then makes the trade that is prohibited by 10b-5. The hacker-seller is effectively aiding and abetting the securities violation committed by the trader; thus, Section 20(e) is a more conducive part of the Exchange Act to prosecute hacker-sellers than 10b-5 is.

Part I of this note traces the history of insider trading law from its origins in the 1933 Securities Act (the Securities Act) and the 1934 Securities Exchange Act. This part places particular emphasis on how insider trading law has gradually stretched the scope of its liability from the classical theory to the misappropriation theory to the even more expansive affirmative misrepresentation theory. Part II distinguishes the hacker-seller as a new type of insider trading culprit that the theories described in Part I are ill-equipped to punish. Part III offers two alternate solutions that would also convict hacker-sellers under the securities laws, but challenges their use because of their ability to be easily abused by prosecutors. Part IV proposes that prosecutors should use the aiding and abetting theory as a more effective way to charge the hacker-seller with insider trading. This part also discusses several policy considerations in support of this theory, and for charging all hackers, including hacker-sellers, under the Securities and

[13] *Dorozhko*, 574 F.3d at 49.

[14] In classical theory cases, the defendant, a corporate insider, owed and breached a fiduciary duty to their own company. In misappropriation theory cases, the defendant owed and breached a fiduciary duty to the source of the information, who may or may not be a corporate insider. Bradley J. Bondi & Steven D. Lofchie, *The Law of Insider Trading: Legal Theories, Common Defenses, and Best Practices for Ensuring Compliance*, 8 N.Y.U. J.L. & BUS. 151, 157–60 (2011).

[15] Securities Exchange Act of 1934, 15 U.S.C. § 78t(e) (2012).

Exchange Act in addition to computer crimes and/or wire fraud statutes. This note concludes that the aider and abettor theory leads to the most effective prosecution of hacker-sellers by the SEC.

I. BACKGROUND ON INSIDER TRADING LIABILITY

The United States Congress enacted the Securities Act in 1933 and the Securities Exchange Act in 1934 in the aftermath of the stock market crash of 1929 amid "reports of widespread abuses in the securities industry."[16] Congress passed these two landmark acts with three objectives in mind: "To provide fair and honest mechanisms for the pricing of securities, to assure that dealing in securities is fair and without undue preferences or advantages among investors, . . . and to provide, to the maximum degree practicable, markets that are open and orderly."[17]

Although commonly understood as the trading of a public company's stock or other securities by individuals with access to nonpublic information about that company, insider trading was not specifically defined in either the 1933 or 1934 Acts.[18] Instead, Section 10(b) of the Exchange Act, along with Rule 10b-5 thereunder (promulgated by the SEC in 1942), proscribe several fraudulent practices "in connection with the purchase or sale of any security."[19] The SEC designed 10(b) as a "catch-all" provision to prevent fraudulent practices within the securities market.[20] Thereafter, these ambiguous statutes were left to the courts for interpretation, who have spent the last seventy-plus years "establish[ing] clear boundaries for prosecution" under the acts,[21] namely defining what type of conduct constitutes insider trading and who can be charged with it.[22] This section illustrates how those boundaries have been stretched by the classical and misappropriation theories of

[16] Cent. Bank of Denver v. First Interstate Bank of Denver, 511 U.S. 164, 170–71 (1994).

[17] H.R. REP. NO. 94-229, at 91–92 (1975).

[18] *See* Securities Act of 1933, 15 U.S.C. § 77b (1934); Securities Exchange Act of 1934, 15 U.S.C. § 78b (1940).

[19] 17 C.F.R. § 240.10b-5 (2016); *see* Securities Exchange Act of 1934, 15 U.S.C. §§ 77b, 78b (2012).

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

[21] 1 BERNARD D. REAMS, JR., INSIDER TRADING AND SECURITIES FRAUD: A LEGISLATIVE HISTORY OF THE INSIDER TRADING AND SECURITIES FRAUD ENFORCEMENT ACT OF 1988, at 9 (1989).

[22] Blue Chip Stamps v. Manor Drug Stores, 421 U.S. 723, 737 (1975) (describing 10b-5, as related to insider trading, as "a judicial oak which has grown from little more than a legislative acorn").

insider trading liability adopted by the Supreme Court, and by the affirmative misappropriation theory introduced by the Second Circuit.

A. *One Step Forward, Two Steps Back: The Classical Theory*

1. The Disclose or Abstain Rule

The cases of *In re Cady, Roberts & Co.*[23] and *SEC v. Texas Gulf Sulphur* canonized the "disclose or abstain" rule that the classical theory stems from.[24] The rule—requiring an insider to disclose material nonpublic information before trading based on such information or abstain from trading if disclosure is not possible—represents the classical theory at its earliest and broadest point.

In *In re Cady, Roberts & Co.*, the SEC found that Gintel, a partner at the brokerage firm of Cady, Roberts & Co., had violated Rule 10b-5 when he sold several shares of Curtiss Wright Company stock after one of its directors, who was also a director of Cady, Roberts, told him about Curtiss Wright's impending dividend cut.[25] In so doing, the SEC articulated what became known as the "disclose or abstain" rule: an insider who possesses material nonpublic information must disclose that information to the proper authorities before trading on it; if they do not disclose, they must abstain from trading.[26]

The Second Circuit formally adopted the "disclose or abstain" rule in *SEC v. Texas Gulf Sulphur Co.,* holding that *anyone* who possesses material nonpublic information about a company must either disclose that information to the investing public or abstain from trading in that company's stock.[27] The court harkened back to the legislative intent of the 1933 and 1934 Acts in its reasoning, explaining that this standard protects the integrity and fairness of the marketplace by ensuring investors have relatively equal access to material information.[28]

The breadth of the disclose or abstain rule adopted in *Texas Gulf Sulphur* meshed well with the all-encompassing language of 10b-5.[29] Congress crafted the statute using ambiguous language that did not define specific conduct as illegal insider trading. This decision gave the SEC a wide net with which it

[23] *In re* Cady, Roberts & Co., No. 8-3925, 40 SEC Docket 907 (Nov. 8, 1961).

[24] SEC v. Tex. Gulf Sulphur Co., 401 F.2d 833, 848 (2d Cir. 1968) (en banc).

[25] *In re Cady, Roberts & Co.*, 40 SEC Docket at 909, 911.

[26] *Id.* at 911.

[27] *Tex. Gulf Sulphur*, 401 F.2d at 848.

[28] *Id.* at 858–60.

[29] *Id.* at 859.

could characterize several types of trading as insider trading violations when done using material nonpublic information.[30] *Texas Gulf Sulphur* paired seamlessly with the statute and expanded the SEC's net even further by holding that anyone would be liable for insider trading under 10b-5 if they did not follow the disclose or abstain rule.[31]

2. The Rise of the Fiduciary Duty Requirement

The disclose or abstain rule lasted a mere twelve years until the U.S. Supreme Court rejected it in *Chiarella v. United States*.[32] Vincent Chiarella worked as a financial printer hired by corporations to fill out paperwork for takeovers.[33] After deciphering code names assigned to several acquisition targets, he purchased shares in the target companies and sold them for significant profits once the tender offers were announced to the public.[34] The Second Circuit convicted Chiarella of insider trading under 10b-5, but the Supreme Court reversed.[35] Writing for the majority, Justice Powell articulated the central tenet of the classical theory: "one who fails to disclose material information prior to . . . a transaction commits fraud only when he is under a duty to do so."[36] Furthermore, "the 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.'"[37] Chiarella's conviction could not stand because "he was not a fiduciary" and therefore did not owe the target shareholders a fiduciary duty to disclose.[38]

Chiarella's fiduciary framework served two key purposes for the Court. First, it dramatically reduced the categories of persons who could be charged under 10b-5, thereby preventing what Justice Powell saw as prosecutorial overreaching by the federal government using the wide net of *Texas Gulf Sulphur*.[39] Second, it allowed for traditional

[30] *Id.*

[31] *Id.* at 848.

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

[33] *Id.* at 224.

[34] *Id.*

[35] *Id.* at 225.

[36] *Id.* at 228.

[37] *Id.* (alteration in original) (quoting RESTATEMENT (SECOND) OF TORTS § 551(2)(a) (AM. LAW INST. 1976)).

[38] *Id.* at 232.

[39] Donald C. Langevoort, *Words from on High About Rule 10b-5:* Chiarella*'s History,* Central Bank*'s Future*, 20 DEL. J. CORP. L. 865, 872 (1995) (explaining how

corporate insiders to continue to be prosecuted if they trade on confidential information for their own financial gain.[40]

Chiarella's fiduciary framework was reaffirmed in *Dirks v. SEC*.[41] Dirks was a security analyst for a broker-dealer firm who learned from Ronald Secrist that Secrist suspected his former employer, Equity Funding of America, of committing securities fraud.[42] He shared his knowledge of the alleged fraud with a number of his clients, thereby tipping them off, and the clients promptly sold their shares to avoid losses.[43] Like Mr. Chiarella, Dirks was not a fiduciary to the shareholders he tipped off, but the SEC attempted to distinguish the two cases by arguing that tippees like Dirks become obligated to disclose the receipt of inside information from a corporate insider to the shareholders.[44] Therefore, in a callback to the pre-*Chiarella* conception of insider trading, the SEC argued that "anyone who knowingly receives nonpublic material information from an insider has a fiduciary duty to disclose before trading."[45]

Writing for the majority again, Justice Powell reversed the SEC's conviction of Dirks under Rule 10b-5 for "tipping" material nonpublic information about Equity Funding of America.[46] The Court disagreed with the SEC holding that its theory was in conflict with the central tenet of *Chiarella*; not everyone who trades on material nonpublic information has a fiduciary duty towards the shareholders to disclose that information.[47] This tenet was refined in *Dirks* to mean that not everyone has an *inherent* fiduciary duty to disclose.[48] The Court held that corporate insiders have an inherent fiduciary duty to disclose material nonpublic information before trading, and they are not allowed to give such information to outsiders who use it for personal profit.[49] Tippees, on the other hand, acquire that fiduciary duty "when the *insider* has breached his fiduciary duty to the shareholders by disclosing the information

Justice Powell "deliberately" crafted the classical theory to curb the government's use of "10b-5 as a general weapon against unfair information advantages").

[40] *See Chiarella*, 445 U.S. at 230 ("Application of a duty to disclose prior to trading guarantees that corporate insiders, who have an obligation to place the shareholder's welfare before their own, will not benefit personally through fraudulent use of material, nonpublic information.").

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

[42] *Id.* at 648–49.

[43] *Id.* at 648–51.

[44] *Id.* at 656.

[45] *Id.*

[46] *Id.* at 657–58.

[47] *Id.* at 655, 658–59.

[48] *Id.* at 659–60.

[49] *Id.*

to the tippee and the tippee knows or should know that there has been a breach."[50] In this way, the tippee's liability is derived from that of the tipper.[51]

The Supreme Court, however, also recognized that not all disclosures by corporate insiders violate the fiduciary duty of shareholders.[52] Echoing a sentiment from *Cady, Roberts* that the securities laws were enacted to eliminate the "use of inside information for personal advantage,"[53] the Court held that only improper disclosures are breaches of fiduciary duty.[54] An improper disclosure, the Court reasoned, was one from which the insider will personally benefit from, directly or indirectly.[55] The Court used this newly invented "personal benefit" requirement to overturn Dirks's conviction, finding that the official who tipped him off did so to expose his employer's fraud instead of trading on the information for personal gain.[56] Accordingly, Dirks could not be prosecuted under 10b-5.[57]

The *Chiarella* and *Dirks* cases premised the classical theory on who was breaching their fiduciary duty rather than on whether the insider's actions constituted that breach.[58] Therefore, the Court felt that it could extend this theory to all people who could be considered insiders, including employees and agents of the corporation.[59] It could not, however, be extended to anyone considered an outsider of the company; therefore, those outsiders could trade on nonpublic information without fear of prosecution under 10b-5.[60]

B. *A Bigger Step Forward: The Misappropriation Theory*

The misappropriation theory is a second, alternate theory of insider trading liability that captures corporate

[50] *Id.* (emphasis added).

[51] *Id.*

[52] *Id.*

[53] *In re* Cady, Roberts & Co., No. 8-3925, 40 SEC Docket 907, 912 n.15 (Nov. 8, 1961).

[54] *Dirks*, 463 U.S. at 660–61.

[55] *Id.*; *see also* Donna M. Nagy, *Insider Trading and the Gradual Demise of Fiduciary Principles*, 94 IOWA L. REV. 1315, 1329–30 (2009) (describing the advent of the "'personal benefit' requirement as sharply distinguish[ing] a fiduciary's breach of the duty of loyalty (which would trigger Rule 10b-5 liability) from a breach of a fiduciary's duty of care (which would not result in a Rule 10b-5 violation)").

[56] *Dirks*, 463 U.S. at 667.

[57] *Id.*

[58] Nagy, *supra* note 55, at 1329–30.

[59] *Dirks*, 463 U.S. at 655 n.14. ("Under certain circumstances, such as where corporate information is revealed legitimately to an underwriter, accountant, lawyer, or consultant working for the corporation, these outsiders may become fiduciaries of the shareholders.").

[60] Nagy, *supra* note 55, at 1330.

outsiders—people who do not work for the company whose securities are illegally traded or people considered temporary insiders under *Dirks*[61]—who trade on the basis of material nonpublic information. Although the Court did not adopt this theory until *United States v. O'Hagan* in 1997, its first interaction with it was in *Chiarella*.[62] In his concurrence, Justice Stevens argued that Mr. Chiarella had violated 10b-5 by breaching a duty of silence that was "unquestionably owed to his employer and to his employer's customers."[63] In essence, Justice Stevens believed Mr. Chiarella was guilty because he had defrauded the acquiring companies who supplied the tender offers and who trusted that same employer to maintain the confidence of that information.[64] Chief Justice Burger advocated the "fraud-on-the-investors" approach,[65] an even broader version of the misappropriation theory than Justice Stevens's "fraud-on-the-source" approach.[66] In Justice Burger's view, Mr. Chiarella did not defraud the companies who supplied the tender offers but, instead, defrauded the investors with whom he traded by exploiting his knowledge of the tender offers—knowledge that the investors lacked.[67] Like Justice Powell, Justice Stevens and Chief Justice Burger did not focus on the conduct that would have amounted to a breach of fiduciary duty and focused instead on the players involved in the transaction. However, they came to opposite conclusions on who was being harmed by the fiduciary's breach. The Court did not decide whether either conclusion could be a viable alternative in *Chiarella*,[68] and before answering that question, it had to first determine whether the misappropriation theory itself was a viable alternative to the classical theory. A circuit

[61] In a footnote to the *Dirks* opinion, Justice Powell listed "an underwriter, accountant, lawyer, or consultant" as examples of temporary insiders. *Dirks*, 463 U.S. at 655 n.14.

[62] *See* Chiarella v. United States, 445 U.S. 222, 228 (1980) (Stevens, J., concurring); *see also* Stephen M. Bainbridge, *Insider Trading Regulation: The Path Dependent Choice Between Property Rights and Securities Fraud*, 52 SMU L. REV. 1589, 1601–02 (1999) (explaining that the theory's roots are commonly traced to *Chiarella*, Bainbridge notes Chief Justice Burger's dissent in *Chiarella* is also thought to be its point of origin, but, as I explain, its actual origins lie in Justice Stevens's concurrence).

[63] *Chiarella*, 445 U.S. at 238 (Stevens, J., concurring).

[64] *Id.*

[65] Nagy, *supra* note 55, at 1330.

[66] In his dissent, Chief Justice Burger argued that the duty to disclose should be triggered "when an informational advantage is obtained, not by superior experience, foresight, or industry, but by some unlawful means." *Chiarella*, 445 U.S. at 240 (Burger, C.J., dissenting).

[67] *Id* at 243–45.

[68] *Id.* at 238 (Stevens, J., concurring).

split emerged over the next seventeen years resulting from that very question.[69]

The Supreme Court resolved the split in *O'Hagan* by formally endorsing the misappropriation theory, but it chose to do so based on Justice Stevens's fraud-on-the-source theory instead of Chief Justice Burger's fraud-on-the-investors theory.[70] James O'Hagan was a partner at a large Minneapolis law firm who learned that one of his firm's clients, Grand Metropolitan, was planning a tender offer for shares of Pillsbury Corporation.[71] O'Hagan subsequently purchased several shares of Pillsbury stock and sold them for $4.3 million after Grand Metropolitan publicized the tender offer.[72] A jury convicted him of insider trading under Rule 10b-5, but the Eighth Circuit overturned the conviction, holding that the misappropriation theory was an invalid premise for 10b-5 liability.[73]

The Supreme Court disagreed and endorsed the misappropriation theory in reversing the Eighth Circuit.[74] Writing for the majority, Justice Ginsburg held that this alternate theory creates 10b-5 liability when a person commits fraud "in connection with the purchase or sale of [a] security" by misappropriating confidential information in order to trade on it, thereby breaching a fiduciary duty owed to the source of the information.[75] In Justice Ginsburg's view, that fiduciary duty, unlike the fiduciary duty owed by corporate insiders under the classical theory, is premised on "a fiduciary-turned-trader's deception of those who entrusted him with access to confidential information."[76] O'Hagan had a duty of trust and confidence to his

[69] In *United States v. Newman*, the Second Circuit agreed with Justice Stevens and affirmed the 10b-5 convictions of employees of an investment banking firm who misappropriated information about potential mergers to three traders and shared the profits made from purchasing the stock of the upcoming merger targets. United States v. Newman, 664 F.2d 12, 16–18 (2d Cir. 1981), *aff'd* 722 F.2d 729 (2d Cir. 1983). The court held that the employees violated a fiduciary duty owed to the source of the merger information, the investment bank and its clients from whom they stole the information. *Id.* By 1991, the Seventh and Ninth Circuits threw their support behind the misappropriation theory, too. *See* SEC v. Cherif, 933 F.2d 403, 410 (7th Cir. 1991); SEC v. Clark, 915 F.2d 439, 453 (9th Cir. 1990). In 1995, however, the Fourth Circuit rejected the misappropriation theory on the grounds that it would hold misappropriators liable without satisfying the deceptive device requirement because there would be no "'misrepresentation' or 'nondisclosure.'" United States v. Bryan, 58 F.3d 933, 949–50 (4th Cir. 1995).

[70] United States v. O'Hagan, 521 U.S. 642, 682 (1997) (Thomas, J., concurring in part and dissenting in part).

[71] *Id.* at 647.

[72] *Id.* at 648.

[73] United States v. O'Hagan, 92 F.3d 612, 614, 617 (8th Cir. 1996), *rev'd by* 521 U.S. 642 (1997), *remanded to* 139 F.3d 641 (8th Cir. 1998).

[74] *Id.* at 655.

[75] *Id.* at 655–56 (alteration in original).

[76] *Id.* at 652.

law firm and, by extension, his firm's clients, and violated that duty by trading on the nonpublic information he obtained for personal gain.[77] The Supreme Court held that his actions satisfied the "deceptive" requirement of Section 10(b).[78]

The Court in *O'Hagan* also advocated the misappropriation theory as a new method to endorse the efficient market policy considerations that underlie the Securities Act and the Securities Exchange Acts.[79] Justice Ginsburg stressed that the 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 th[e] corporation's security price when revealed."[80] This protection, she reasoned, would promote investor confidence because investors would be reluctant to trade in a market where the use of misappropriated nonpublic information is "unchecked by law."[81]

The Court in *Chiarella* restricted insider trading liability to corporate insiders who owe a fiduciary duty to the source of material nonpublic information.[82] *O'Hagan* expanded the range of activities that give rise to that fiduciary duty, and in so doing, expanded the class of insider trading defendants to include corporate outsiders that misappropriate nonpublic information "in connection with" securities transactions.[83] But the Court declined to expand insider trading liability to those who lack a "fiduciary-like nexus" to the source.[84] In the modern age it is precisely these outsiders, particularly hacker-sellers, that present the greatest threat to the market because they do not need to have a connection with the source of the material nonpublic information to obtain it.

C. Expansion to "True" Outsiders: The Affirmative Misrepresentation Theory

A critical question in the wake of the *O'Hagan* decision was whether the misappropriation theory actually applied to true outside traders, those who did not owe a fiduciary duty to the source of the information. The Second Circuit's decision in *SEC v. Dorozhko* provided an answer that question; its opinion

[77] *Id.* at 659.

[78] *Id.*

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

[80] *Id.* at 653 (alterations in original) (quoting Brief for the United States at 14, United States v. O'Hagan, 521 U.S. 642 (1997) (No. 96-842)).

[81] *Id.* at 658–59.

[82] *See* Chiarella v. United States, 445 U.S. 222, 232 (1980).

[83] *O'Hagan*, 521 U.S. at 655.

[84] Nagy, *supra* note 55, at 1320.

simultaneously limited the scope of the misappropriation theory and created a new complimentary theory—known as the affirmative misrepresentation theory—that was not premised on a breach of fiduciary duty.[85]

The facts of the case are a good example of a true outsider whose 10b-5 liability was not considered by the *O'Hagan* court. In early October 2007, IMS Health, Inc., announced that it would release its third-quarter financials on October 17, at 5:00 p.m., and Thomson Financial, Inc. would manage the release.[86] On that afternoon, Oleksandr Dorozhko—a Ukrainian citizen—hacked into a server at Thomson Financial, stole the IMS Health earnings report set to be released at 5:00, and subsequently bought $41,670.90 worth of put options of IMS Health stock.[87] The next day, after IMS Health released its lower-than-expected third-quarter earnings, Dorozhko sold the put options six minutes after the opening bell for a profit of $286,456.59.[88] The United States District Court for the Southern District of New York denied the SEC's request for a preliminary injunction to prevent Dorozhko from accessing his newly acquired profit.[89] The court held that "computer hacking was not 'deceptive'" because it did not have the requisite breach of a fiduciary duty of disclosure.[90] Dorozhko had no affiliation with either IMS Health or Thomson Financial and, therefore, had no fiduciary duty to disclose.[91] Because there was no fiduciary duty, there was no breach.[92]

On appeal, the Second Circuit Court of Appeals reversed the district court, finding that computer hacking could be considered a deceptive device under 10(b).[93] Controversially, the court also held that breaching a fiduciary duty of disclosure was not a requirement for insider trading liability, saying, "what is sufficient [to prove liability under 10b-5] is not always what is necessary."[94] The Second Circuit distinguished *Dorozhko* from the Supreme Court precedent that the district court relied on, stating that those cases involved fraud based on a breach of fiduciary duty of disclosure.[95] Finding that no such duty existed

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

[86] *Id.* at 44.

[87] *Id.*

[88] *Id.*

[89] *Id.* at 45 (citing SEC v. Dorozhko, 606 F. Supp. 2d 321, 330 (S.D.N.Y. 2008)).

[90] *Id.*

[91] *Dorozhko*, 606 F. Supp. 2d at 330.

[92] *Id.*

[93] *Dorozhko*, 574 F.3d at 51.

[94] *Id.* at 49.

[95] *Id.* at 48–50.

for Dorozhko in the case at bar, the court agreed with the SEC and characterized Dorozhko's actions as fraud based on affirmative misrepresentation.[96] Essentially, Dorozhko misrepresented himself to access Thomson Financial's computer system, appearing as a person who could legally access the earnings report but who in reality had no such permission to do so.[97]

The court also discussed the relevance of Dorozhko's method of hacking to his liability under 10b-5.[98] It held that if a person misrepresents his identity to gain access to a server and then steals information off of the server to trade on it, those actions would be "plainly 'deceptive' within the ordinary meaning of the word" and thus prohibited by 10b-5.[99] However, the court remanded the question of whether "exploiting a weakness in an electronic code to gain unauthorized access is 'deceptive'" and prohibited by 10b-5 to the district court.[100] On remand, the SEC moved for and was granted summary judgment, and the question was never answered.[101]

As in *Chiarella*, *Dirks*, and *O'Hagan*, the deciding court also bolstered its new theory of insider trading with policy considerations. The Second Circuit stated that the affirmative misrepresentation theory is consistent with "the Supreme Court's oft-repeated instruction that Section 10(b) 'should be construed not technically and restrictively, but flexibly to effectuate its remedial purposes.'"[102] It is unlikely that the authors of the Security Act and the Securities Exchange Act contemplated Dorozhko's actions, but it is likely that they crafted the acts with broad enough language to imbue 10b-5 liability on him nonetheless.[103]

The classical, misappropriation, and affirmative misrepresentation theories have stretched the boundaries of insider trading liability well beyond its original restriction to corporate insiders. Of the three theories, the last is perhaps the broadest and most aggressive expansion of insider trading

[96] *Id.* at 49–51.

[97] *Id.* at 44, 49.

[98] *Id.*

[99] *Id.* at 51.

[100] *Id.*

[101] SEC v. Dorozhko, Release No. 21465, 2010 WL 1213430 (Mar. 29, 2010).

[102] *Dorozhko*, 574 F.3d at 49 (quoting SEC v. Zandford, 535 U.S. 813, 819 (2002)).

[103] Alan Turing, often considered the father of modern computers, did not write the paper that first described the principles of modern computing until 1936. A.M. Turing, *On Computable Numbers, with an Application to the Entscheidungsproblem*, 42 PROC. LONDON MATHEMATICAL SOC'Y 230, 230–65 (1936). The Securities Act was promulgated in 1933, and the Securities Exchange Act in 1934.

liability.[104] By abandoning the fiduciary realm of the classical and misappropriation theories, the affirmative misrepresentation theory expands liability to true outsiders who lack the "fiduciary like nexus" required by those theories.[105] Dorozhko is an example of such an outsider, a hacker who had no fiduciary allegiance to the company whose information he stole, IMS Health, or to the company that housed the information that he stole, Thomson Financial.[106] His liability, therefore, falls outside of the classical and misappropriation theories because it cannot be premised on their fiduciary principles; he is, however, liable under the affirmative misrepresentation theory because he fraudulently misrepresented himself as a person who could legally access the inside information held by Thomson Financial when he hacked into the server. As the next part demonstrates, however, the affirmative misrepresentation theory does not capture all types of computer hacking.

II. A NEW APPROACH TO AN OLD CRIME: WHY THE HACKER-SELLER DOES NOT FIT UNDER THE THREE MAJOR THEORIES OF INSIDER TRADING LIABILITY

Although the advent of the classical, misappropriation, and affirmative misrepresentation theories expanded the limits of insider trading liability, the case of the hacker-seller falls outside the domain of those theories for three reasons. First, they do not owe a fiduciary duty toward either the corporation or the source of the material nonpublic information. Second, the holding in *Dorozhko* only creates liability for hacking that is considered "plainly 'deceptive.'"[107] It correctly implies, however, that not all hacking fits that mold; as such, the hacker-seller's liability under 10b-5 must turn on whether the method of hacking is deceptive under 10b-5. Third, and most importantly, the hacker-seller's conduct does not directly relate to, (i.e., is not "in connection with"), the unlawful securities transaction because they do not actually trade on the information they acquire. These three reasons indicate that 10b-5 is not the proper part of the Exchange Act with which to charge hacker-sellers for insider trading. Instead, Section 20(e), the aiding and abetting provision of the Exchange Act, is a more effective provision with which to charge hacker-sellers.

[104] Donna M. Nagy, *Reframing the Misappropriation Theory of Insider Trading Liability: A Post-*O'Hagan *Suggestion*, 59 OHIO ST. L.J. 1223, 1251–56 (1998).

[105] Nagy, *supra* note 55, at 1320.

[106] *Dorozhko*, 574 F.3d at 49–51.

[107] *Id.* at 51.

A. Hacker-Sellers Are Not Fiduciaries

The classical theory of insider trading premises 10b-5 liability on a corporate insider's breach of fiduciary duties owed to the corporation and its shareholders by trading on material nonpublic information or failing to disclose such information before trading.[108] Hacker-sellers do not work for the corporation whose information they trade on or sell; as such, they are not corporate insiders and owe no fiduciary duty to the corporation or to its shareholders.[109] Therefore, hacker-sellers cannot be liable under the classical theory.

The absence of fiduciary duty manifests differently in the misappropriation theory. In *O'Hagan*, the Supreme Court premised the misappropriation theory on the breach of a fiduciary duty owed to the source of the information. A misappropriator's "deception" occurs when he or she feigns "loyalty to the principal while secretly converting the principal's information for personal gain."[110] All hackers, including hacker-sellers, cannot be held under this standard because they have no loyalty to the source of the information.[111] They never agree to maintain the confidence of the source's information because they never transact with the source from which they acquire the information. In fact, the hacker-seller often does not even acquire the information from the would-be-source itself.[112] Put simply, there is no relationship between the hacker-seller and the source that gives rise to a fiduciary duty owed by the former to the latter; therefore, hacker-sellers also cannot be liable under the misappropriation theory.

B. Not All Hacking Is "Plainly Deceptive"

While the previous section demonstrates how it is relatively simple for hacker-sellers to evade liability under the classical and misappropriation theories, it is more difficult for them to escape the affirmative misrepresentation theory. While the *Dorozhko* court's discussion of deceptive conduct under the affirmative misrepresentation theory is a step in the right direction, it left several cracks for hacker-sellers to slip through. This section picks up where the Second Circuit left off by

[108] *See* Chiarella v. United States, 445 U.S. 222 (1980) (holding that liability under the classical theory is premised on an insider's fiduciary duty to disclose material nonpublic information).

[109] *Dorozhko*, 574 F.3d at 49.

[110] United States v. O'Hagan, 521 U.S. 642, 653 (1997) (quoting Brief for the United States, *supra* note 80, at 17).

[111] Nagy, *supra* note 104, at 1253–54.

[112] *See, e.g.*, *Dorozhko*, 574 F.3d at 43–44.

qualifying its rudimentary distinction between misrepresenting oneself to a computer and exploiting a structural weakness. The court strongly implied that not all hacking would be considered deceptive conduct but did not answer what conduct would or would not be deceptive.[113] The court correctly pointed out that hacking involving affirmative misrepresentations to the computer does carry 10b-5 liability, but hacking that exploits structural deficiencies cannot carry 10b-5 liability because the computer is not being "deceived" by the hack. As such, the affirmative misrepresentation theory only applies to a subset of hackers, regardless of whether they trade on the information themselves or sell it to others and is, therefore, inadequate in imbuing liability on hacker-sellers.

1. Misrepresentative Hacking Versus Structural Hacking

Say Corporation *X* keeps its earnings reports in a combination safe in the basement of its headquarters until they are released to the public. Tanya Trader, an independent trader, wants to acquire this information before it becomes public so she can trade on it, but since she does not know how to break into *X*'s safe to get the reports she hires Harry Hacker, a professional safecracker, to do it for her. Harry has two ways to break into the safe. He can misrepresent himself and appear as a legitimate entrant by obtaining the combination and entering it, thereby making the safe grant him access to its contents. Alternatively, Harry can exploit structural weaknesses in the safe by drilling into it, blowing its doors off, or stealing the entire physical object to acquire the information. Harry and Tanya get the information they desire regardless of which option Harry chooses; however, Harry would only be liable for insider trading under the affirmative misrepresentation theory for the former conduct because Harry is deceiving the system into granting him legitimate access. In the digital world, Harry's two options are also present, but manifest themselves in different ways.

a. Misrepresentative Hacking

Misrepresentative computer hacking describes conduct where the hacker attempts to gain access to the computer or information system by hiding his true identity and appearing as a legitimate user. There are several ways the hacker can do

[113] *Id.* at 51.

this, including password cracking, phishing, viruses, worms, and Trojan horses.

Password cracking is the process of recovering passwords from data that has been stored or transmitted by a computer system.[114] The hacker runs a program that repeatedly checks possible combinations against a custom character set until it finds the right one. A common and extremely effective example of password cracking is brute force, where the computer program tries every type of password until it succeeds.[115] The time it takes to crack a password is proportional to bit strength,[116] which is the estimate of the average number of times an attacker who does not have direct access to the password would need to guess it correctly.[117] Once the hacker gets the correct password, the computer will grant him access as though he were a legitimate user.

Phishing is the attempt to acquire sensitive information by masquerading as a trustworthy entity in an electronic communication.[118] The hacker typically sends a seemingly benign email, or "hook," that victims receive directing them to a fraudulent website where they are tricked into divulging sensitive information by displaying messages such as "verify your account" or "confirm billing information."[119] The fraudulent websites will be crafted to look exactly like the real ones, and the user will be deceived into thinking the prompts are legitimate when they are not. Essentially, the fake websites are "bait" set by the hacker to get a user, the "fish," to reveal private information.

Viruses and worms are harmful computer programs that modify other computer programs to replicate the virus or worm repeatedly until the computer crashes. Once the program enters the computer, it secretly prompts the computer's operating system to add a copy of the virus or worm to the target program.[120] The only difference between viruses and worms is that the virus requires human action to infect the computer; worms infect using a computer network, without human input.

[114] WILLIAM E. BURR ET AL., NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, ELECTRONIC AUTHENTICATION GUIDELINE 104 (2013).

[115] *Brute Force Attack*, TECHOPEDIA, https://www.techopedia.com/definition/18091/brute-force-attack [https://perma.cc/CC7L-PEFZ].

[116] BURR ET AL., *supra* note 114, at 104–05.

[117] *Security Tip (ST04-002): Choosing and Protecting Passwords*, US-CERT (May 21, 2009), https://www.us-cert.gov/ncas/tips/ST04-002 [https://perma.cc/2U7F-NZDR].

[118] Zulfikar Ramzan, *Phishing Attacks and Countermeasures*, *in* HANDBOOK OF INFORMATION AND COMMUNICATION SECURITY 433–34 (Peter Stavroulakis & Mark Stamp eds., 2010).

[119] *Id.*

[120] Peter J. Denning, *Computer Viruses*, *in* COMPUTERS UNDER ATTACK: INTRUDERS, WORMS, AND VIRUSES 285–87 (Peter J. Denning ed., 1990).

In the securities context, the virus or worm is harmful when it contains a payload, or code designed to exfiltrate data from the host computer.[121] The hacker dupes the user into allowing the virus or worm to enter the computer by using tactics such as phishing to make the message containing the virus or worm seem harmless.[122] Once the virus or worm has entered the computer, it launches the payload to steal sensitive information from the user.

Trojan horses misrepresent themselves as useful or routine in order to persuade a user to install it.[123] Like viruses or worms, Trojan horses are generally spread by some form of social engineering[124] where the user is duped into opening the device—usually an email—that contains it.[125] Their ability to steal a user's information once on the system depends on the type of Trojan.[126] For example, password-stealing Trojans look for saved passwords on the user's computer and then email them to the perpetrator.[127]

Password cracking, phishing, viruses, worms, and Trojan horses are all forms of misrepresentative hacking because the hacker must appear legitimate to the user or computer in order for these techniques to be successful. The hacker employs password cracking or phishing to acquire the correct password and then enters the system by logging in with the correct information. The computer believes the hacker is a legitimate user because the correct information was entered, so it grants the hacker access. Similarly, the hacker appears as a legitimate entity when employing a virus, worm, or Trojan horse by disguising the malware in seemingly benign emails or websites; the users are tricked into opening the email or interacting with the website because they think it looks safe.[128] In either case, the hacker is

[121] *Payload*, TECHOPEDIA, https://www.techopedia.com/definition/5381/payload [https://perma.cc/MN52-ZWFX].

[122] *What Is the Difference: Viruses, Worms, Trojans, and Bots?*, CISCO, http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html [https://perma.cc/YD5N-WEWW].

[123] CARL E. LANDWEHR ET AL., NAT'L RESEARCH LAB., A TAXONOMY OF COMPUTER PROGRAM SECURITY FLAWS, WITH EXAMPLES 7 (1993).

[124] Social engineering is "the art of manipulating people so they give up confidential information." *What Is Social Engineering?*, WEBROOT, https://www.webroot.com/us/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering [https://perma.cc/58K7-JPVQ]. Criminals or hackers use different tricks to masquerade as harmless people—such as pretending to be a known friend of the user or sending the user an email saying they won a contest—and ask the user to provide confidential information. *Id.* By posing as someone the user trusts, the user is more inclined to divulge sensitive information. *Id.*

[125] *See supra* sources cited in notes 122–123.

[126] Robert Siciliano, *What Is a Trojan Horse?*, INTEL SEC. (Oct. 27, 2014), https://blogs.mcafee.com/consumer/trojan-horse/ [https://perma.cc/Q9Q2-2LQG].

[127] *Id.*

[128] LANDWEHR ET AL., *supra* note 123, at 7.

misrepresenting his identity to the target to acquire sensitive information; he is appearing as a legitimate entity to the computer when, in fact, he is not.

It is this form of hacking that Dorozhko used to acquire information about IMS Health's earnings from Thomson Financial.[129] He deceived the Thomson Financial security system by appearing as a legitimate user who had authorized access to the confidential information about IMS Health.[130] As such, Dorozhko's conduct was deceptive under 10b-5.

b. Structural Hacking

Structural hacking describes conduct where the hacker exploits structural deficiencies in the computer to obtain valuable information contained within. Like misrepresentative hacking, there are several ways this can be done, such as physical exploitation or code injections.

Not all hacking occurs digitally; "you can spend millions of dollars protecting your network, but [many organizations] are leaving the front door wide open."[131] It is often just as effective for hackers to exploit physical components of the networks or the facilities themselves to acquire the information they desire.[132] The physical design flaws in the rooms where the data is stored, such as raised floors built for running cables and cooling apparatuses, can easily be subjugated.[133] Or perhaps, if they are bold enough, the hacker can walk through the unlocked front door.[134]

Code injections are attacks in which hackers inject malicious code into computer programs that override the programs so they act according to the hacker's wishes.[135] A common type of injection is the Structured Query Language

[129] Posthearing Memorandum of Law at 4, 8, SEC v. Dorozhko, 606 F. Supp. 2d 321 (S.D.N.Y. Dec. 5, 2007) (No. 1:07-CIV-09606 (NRB)).

[130] *Id.* at 4.

[131] Kelly Jackson Higgins, *Five Ways to (Physically) Hack a Data Center*, DARKREADING (May 17, 2010), http://www.darkreading.com/five-ways-to-(physically)-hack-a-data-center/d/d-id/1133615 [https://perma.cc/KL7F-3PC9] (alteration in original) (quoting Ryan Jones, senior security consultant with Trustwave's SpiderLabs).

[132] *Id.*

[133] *Id.*

[134] *See, e.g.*, Steve Ragan, *Hackers Suggest They Had Physical Access During Attack on Sony Pictures*, CSO (Nov. 25, 2014), http://www.csoonline.com/article/2851649/physical-security/hackers-suggest-they-had-physical-access-during-attack-on-sony-pictures.html [http://perma.cc/EY4D-5N38] (discussing the ramifications of allegations that the hackers who broke into Sony's network had physical access because the network never locks the doors to its actual databases and may have had inside help).

[135] Raghunathan Srinivasan & Partha Dasgupta, *Towards More Effective Virus Detectors*, ARIZ. STATE UNIV., http://cactus.eas.asu.edu/partha/Papers-PDF/2007/raghu-csi.pdf [https://perma.cc/3VRT-ZMDS].

(SQL) injection.[136] SQL is the standard operating language in most computers that helps users navigate information databases on all computing platforms. An SQL injection attacks vulnerabilities in this language[137] by inserting a certain predesigned malicious code that manipulates the SQL to grant the hacker unauthorized access.

Neither physical hacking nor SQL injections require the hacker to misrepresent his identity to the computer or system in order to gain unauthorized access. In fact, there is no need for misrepresentation because the hacker does not attempt to appear legitimate at all. Unlike misrepresentative hacks where the hacker must trick the system into believing that nothing is wrong because they are entering as seemingly legitimate users, in structural hacks the system is aware that something is wrong, but is powerless to fix the problem.

2. Misrepresentative and Structural Hacking Under *Dorozhko*

Dorozhko hinted that hacking can be divided into these two groups of conduct: misrepresentative hacking and structural hacking. As this note argues, however, only misrepresentative hacking gives rise to 10b-5 liability because the hacker impersonates someone with legitimate access to the information when he interacts with the computer, thereby satisfying the deceptive device element of the statute. This analysis could acquit hacker-sellers if they used structural hacking to acquire the material nonpublic information, but cases like *SEC v. Dubovoy* demonstrate that this is clearly not always the case. The hackers in *Dubovoy* satisfied the deceptive device requirement when they used password-based hacking to acquire nonpublic press releases.[138] However, they also hacked several times using SQL injections, and this conduct did not involve a deceptive device because they were exploiting structural deficiencies instead of misrepresenting their identities to appear as legitimate users.[139] Therefore, these latter instances of hacking do not give rise to 10b-5 liability because the deceptive

[136] *See* Mike Chapple, *What Is SQL?: Introduction to the Structured Query Language*, THOUGHTCO. (Dec. 11, 2016), https://www.thoughtco.com/what-is-sql-1019769 [https://perma.cc/8D2G-R5PZ].

[137] STEPHEN KOST, INTEGRITY CORP., AN INTRODUCTION TO SQL INJECTION ATTACKS FOR ORACLE DEVELOPERS 4–6 (2004); *see also* Sumner Lemon, *Mass SQL Injection Attack Targets Chinese Web Sites*, IDG NEWS SERV. (May 19, 2008), http://www.pcworld.com/article/146048/article.html [https://perma.cc/FS6P-ZFGA].

[138] Complaint for Violations of the Federal Securities Laws, *supra* note 2, at 21–22.

[139] *Id.*

device requirement is not satisfied. While the distinction between the two types of hacking is important, it can only partially exculpate hacker-sellers depending on the type of hacking they employ.

C. *Why Charging Hacker-Sellers Under 10b-5 Stretches the "In Connection With" Requirement Too Far*

In *Chiarella*,[140] *O'Hagan*,[141] and *Dorozhko*,[142] 10b-5's requirement that the criminal must use a deceptive device "in connection with" the sale of securities was satisfied because the defendant used the deceptive device to acquire material nonpublic information and then traded on that information himself. In the case of a hacker-seller, the connection is much less apparent because the same person did *not* perpetrate the deceptive act and the securities transaction. 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. The previous part of this note demonstrated that hacker-sellers are partially exculpated from 10b-5 liability based on the type of hack they carried out. By contrast, hacker-sellers fail to satisfy the "in connection with" requirement regardless of the type of hack they employ because they do not subsequently trade on the information they acquire.

In *O'Hagan*, the Court construed the "in connection with" requirement to mean that the "fraud is consummated, not when the fiduciary gains the confidential information, but [rather] when . . . the information [is used] to purchase or sell securities."[143] "This hurdle is necessary" in misappropriation cases because the investor's breach of fiduciary duty to his source occurs not when he acquires the information, but when he uses it to purchase or sell securities.[144] Affirmative misrepresentation cases differ because "the fraudulent act is the misrepresentation itself";

[140] Chiarella v. United States, 445 U.S. 222 (1980) (explaining how the defendant deciphered codes about potential tender offers and then purchased securities in those companies before the offers were announced).

[141] United States v. O'Hagan, 521 U.S. 642, 653 (1997) (explaining how the defendant learned of the tender offer his firm had planned and then bought the target company's stock before the offer was announced).

[142] SEC v. Dorozhko, 574 F.3d 42, 44 (2d Cir. 2009) (explaining how the defendant hacked into Thomson Financial to acquire IMS press releases about its earnings report and subsequently bought options in IMS before the report was released to the public).

[143] *O'Hagan*, 521 U.S. at 656.

[144] Elizabeth A. Odian, Note, SEC v. Dorozhko*'s Affirmative Misrepresentation Theory of Insider Trading: An Improper Means to a Proper End*, 94 MARQ. L. REV. 1313, 1337 (2011).

the perpetrator does not need to trade on the acquired information to complete the fraud.[145] However, the perpetrator is not liable under 10b-5 at this point because the fraud has not yet occurred "in connection with" a securities transaction—i.e., the trade on the basis of the nonpublic information has not yet occurred.

It follows that 10b-5 liability must attach in affirmative misrepresentation cases when the perpetrator actually trades on information acquired via an affirmative misrepresentation.[146] The perpetrator would also not be liable under 10b-5 if he chose not to purchase or sell securities because his fraudulent conduct of affirmatively misrepresenting his identity would not have occurred "in connection with" a securities transaction. In the hacker-seller paradigm, the hacker-seller acquires the material nonpublic information, but sells that information to another person to trade on instead of making the trade himself. Because the hacker-seller does not make a trade, he does not engage in any conduct in which 10b-5 liability attaches under the affirmative misrepresentation theory. On the other hand, the affirmative misrepresentation theory does create liability for hacker-traders like Dorozhko who actually trade on the basis of the stolen information.[147]

If courts wanted to find hacker-sellers liable under the affirmative misrepresentation theory, they would have to stretch the "in connection with" requirement beyond current case law to include the purchase or sale of securities *by another person*: the trader. In other words, the hacker-seller's 10b-5 liability would not be premised on his or her own conduct, but on the recipient's. Because the "in connection with" requirement is only premised on the hacker-seller's own conduct, and the hacker-seller does not personally trade on the nonpublic information acquired, the hacker-seller cannot be charged under 10b-5.

III. ALTERNATE SOLUTIONS

This note argues that the aiding and abetting theory is the most effective way to charge hacker-sellers with violating the securities laws. But the aiding and abetting theory is not the only way to charge hacker-sellers. The SEC has other options at

[145] *Id.* at 1338.

[146] *Dorozhko*, 574 F.3d at 48–49.

[147] On October 17, 2017, Dorozhko hacked into a server at Thomson Financial, stole IMS Health's earnings report, and bought approximately $41,670.90 worth of put options of IMS Health stock. *Id.* at 44. The next day, after the earnings were made public, Dorozhko sold the put options six minutes after the opening bell for a profit of $286,456.59. *Id.*

its disposal; these options, however, are more controversial because they could easily be manipulated to expand the net of insider trading liability too far.

A. *Single Scheme Liability: The "In Connection With" Requirement Revisited*

The hacker-seller, by his actions, does not directly satisfy the "in connection with" requirement of 10b-5 because he does not actually commit the securities transaction using the acquired nonpublic information.[148] However, the Supreme Court examined this element of 10b-5 in terms of independent events in *SEC v. Zandford*,[149] and its analysis lends itself to the case of the hacker-seller quite nicely. In *Zandford*, the Court rejected the respondent's claims that his selling of his customer's securities and making personal use of the proceeds was, while fraudulent, not sufficiently "in connection with" a securities transaction because he only misappropriated the customer's assets and not particular securities.[150] Justice Stevens, in his majority opinion, found that the securities sales and Zandford's conversion of the proceeds were not independent events but were done together in furtherance of Zandford's single scheme of defrauding his customer.[151]

Hacker-sellers present a comparable situation because they do not actually commit the securities transaction, but hack in furtherance of a single scheme to commit securities fraud, which is perpetrated by the trader. Here, the key to linking the hacker-seller to the securities violation is to prove that the hacker's actions and the trader's actions are part of a single scheme. Courts would have to do this on a case-by-case basis using an extensive factual inquiry. Facts the court should look for include the proximity of the hacker's acquisition of the nonpublic information to the trader's securities transaction, the independent value, if any, of the information obtained by the hacker-seller,[152] and the method of the trader's payment to the hacker-seller.[153]

[148] *See supra* Section II.C.

[149] SEC v. Zandford, 535 U.S. 813, 820 (2002).

[150] *Id.*

[151] *Id.*

[152] The hacker-seller's conduct would be more connected with the transaction than when the nonpublic information has little value outside of its utility in securities trading. *Id.* at 824.

[153] It would be more indicative of a single scheme if the hacker-seller got paid with a cut of the proceeds from the illicit trade instead of a flat fee at the onset. This would imply that the hacker-seller was fully aware of what the trader was going to do and speaks to their partnership in the securities violation.

B. *Treating the Hacker-Seller as a Tipper*

Tipper-tippee liability has been applied in both the classical and misappropriation theories of insider trading liability on the basis that the tipper breached a fiduciary duty by providing inside information to the tippee, and the tippee knew or had reason to know that the tipper breached that duty.[154] In other words, the tipper's "deceptive device" was the fiduciary breach, which was used "in connection with" a securities transaction perpetrated by another person, the tippee.[155] It is conceivable then that the tipper/tippee paradigm could be expanded beyond its fiduciary restraints to capture tippers that employ any deceptive device in tipping nonpublic information. The hacker-seller would fall under this new net because he is, in effect, tipping the material nonpublic information to the trader. And the tippee in this case would be well aware that the tipper employed the deceptive device because the buyer is paying the hacker-seller for the information with which he will commit the securities violation. This new, wider net would still be in line with the policy considerations from *Dirks* because it captures tippees that "participa[te] after the fact"—i.e., after the tipper employs the deceptive device.[156]

C. *Casting Too Big of a Net: A Warning from* Texas Gulf Sulphur

A crucial problem with alternatives *A* and *B* is that they are sizeable extensions of well-grounded avenues of insider trading liability that could cast too wide of a net and reel in too many potential defendants beyond the hack-sell context. Since *Texas Gulf Sulphur*, courts have espoused their trepidations that the securities laws can easily be abused if their reach is unduly protracted.[157] These concerns are only magnified by the

[154] Dirks v. SEC, 463 U.S. 646 (1983) (application of tipper/tippee liability under the classical theory of 10b-5); United States v. Libera, 989 F.2d 596, 600 (2d Cir. 1993) (application of tipper/tippee liability under the misappropriation theory of 10b-5). The personal benefit requirement from *Dirks* has not been adopted in every misappropriation case. *See* SEC v. Yun, 327 F.3d 1263, 1277–79 (11th Cir. 2003) (accepting the personal benefit requirement because disclosure without it is not sufficient for liability under 10b-5); *Libera*, 989 F.2d at 600 (suggesting that the personal benefit requirement is not necessary because it is implied that the tipper will benefit from tipping the tippee).

[155] *Dirks*, 463 U.S. 646 (application of tipper/tippee liability under the classical theory of 10b-5); *Libera*, 989 F.2d at 600 (application of tipper/tippee liability under the misappropriation theory of 10b-5).

[156] *Dirks*, 463 U.S. at 667 (quoting Chiarella v. United States, 445 U.S. 222, 230, n.12 (1980)).

[157] SEC v. Tex. Gulf Sulphur Co., 401 F.2d 833, 867–70 (2d Cir. 1968) (Friendly, J., concurring) (discussing the ramifications of expansive insider trading

expansion of the securities laws beyond their classical roots. Alternative *B*, the tipper/tippee solution, is more prone to this issue than alternative *A*, because tipper-tippee liability, even in its original incarnation, lends itself to expansive application, particularly with regard to the personal benefit requirement.[158] In *United States v. Salman*, for example, the government argued unsuccessfully before the Supreme Court that "a tipper personally benefits whenever the tipper discloses confidential trading information for a noncorporate purpose."[159] This would mean that a gift to *anyone*—be it friend, family, coworker, etc.,—would satisfy the *Dirks* personal benefit requirement.[160] Although the Supreme Court rejected this argument, it is a powerful demonstration of how wide a net the personal benefit requirement can potentially cast.

IV. AN OLD SOLUTION TO A NEW CRIME: WHY AIDING AND ABETTING LIABILITY EFFECTIVELY CAPTURES THE HACKER-SELLER

The classical, misappropriation, and affirmative misrepresentation theories all premise 10b-5 liability on the perpetrator actually employing a deceptive device in executing a securities transaction. Part II demonstrated the inability of those theories to convict the hacker-seller; while the hacker-seller may use a deceptive device, it will never be "in connection with" a securities transaction because hacker-sellers do not trade on the basis of the information themselves. Their conduct more closely resembles a facilitation of insider trading than actual insider trading, and charging hacker-sellers with aiding and abetting insider trading under Section 20(e) of the Securities Exchange Act is therefore more effective than charging them with directly committing insider trading under 10b-5.

liability and characterizing them as "frightening"); *see also* Blue Chip Stamps v. Manor Drug Stores, 421 U.S. 723, 737 (1975) (warning against the dangers of "vexatious [securities fraud] litigation").

[158] Donald C. Langevoort, *The Demise of* Dirks*: Shifting Standards for Tipper-Tippee Liability*, INSIGHTS, June 1994, at 24; *see also* Kathleen Coles, *The Dilemma of the Remote Tippee*, 41 GONZAGA L. REV. 181, 217 (2005–2006) (arguing that the more remote the tippee, it is "likely that the tippee is being prosecuted for mere possession of confidential information because of the absence of the requisite knowledge of the breach of duty").

[159] Salman v. United States, 137 S. Ct. 420, 426–27 (2016).

[160] *Id.* at 427.

A. Aiding, Abetting, and the Securities Exchange Act

Congress expressly provided for prosecution of those who aid and abet violators of the securities laws in the 1934 Securities Exchange Act.[161] Section 20(e) allows for prosecution of one who "knowingly or recklessly provides substantial assistance to another person in violation of a provision of this chapter, or of any rule or regulation issued under this chapter" by the SEC and they will be held just as culpable as the person to whom they provide assistance.[162] Put another way, in order to aid and abet, one must seek "by his actions to make [the underlying crime] succeed."[163] Over the next six decades, almost every circuit court of appeals endorsed a tort-law based methodology for analyzing the validity of civil liability for aiding and abetting.[164] This approach requires the plaintiff to prove (1) that there was a primary violation of the securities act by a third party; (2) that the alleged aider and abettor must have knowledge of the primary violation; and "(3) 'substantial assistance' by the alleged aider-abettor in achievement of the primary violation."[165]

In *Central Bank of Denver v. First Interstate Bank of Denver*, the Supreme Court denied the applicability of this test to private rights of action.[166] In his majority opinion, Justice Kennedy demonstrated that Congress had "taken a statute-by-statute approach to civil aiding and abetting liability," and pointed out that Congress did not expressly provide for a private aiding and abetting cause of action in the Securities

[161] Securities Exchange Act of 1934, 15 U.S.C. § 78t(e) (2012).

[162] *Id.*

[163] *In re* Amaranth Nat. Gas Commodities Litig., 730 F.3d 170, 182 (2d Cir. 2013) (quoting United States v. Peoni, 100 F.2d 401, 402 (2d Cir. 1938)).

[164] Sean G. Blackman, Comment, *An Analysis of Aider and Abettor Liability Under Section 10(b) of the Securities Exchange Act of 1934:* Central Bank of Denver v. First Interstate Bank of Denver, 27 CONN. L. REV. 1323, 1347–48 n.155 (1995) (listing the accepted theories of aiding and abetting liability as securities violations from all eleven circuit courts); *see also* RESTATEMENT (SECOND) OF TORTS § 876(b) (AM. LAW INST. 1979) (This provision of the Restatement is the tort-law basis from which the circuit courts derived the aiding and abetting theories they endorsed.).

[165] Blackman, *supra* note 164, at 1347–48 n.155.

[166] 511 U.S. 164 (1994). Central Bank of Denver was a trustee for a bond issued by the Colorado Springs-Stetson Hills Public Building Authority. *Id.* at 167. The bonds required that the underlying securities must be worth at least 160% of the total outstanding principal and interest on the bond and that AmWest Development give Central Bank an annual report confirming that valuation. *Id.* After becoming aware that the test was not being met, Central Bank was advised by AmWest to wait to review the underlying securities themselves until after the bonds were issued. *Id.* at 167–68. Before Central Bank could perform the review, Colorado Springs defaulted on the bonds. *Id.* at 168. First Interstate Bank, the buyer of the bonds, sued AmWest and Central Bank, alleging that Central Bank aided and abetted AmWest's fraud under 10b-5. *Id.*

Exchange Act but had included one in other statutes created at the same time.[167] Based on this, Justice Kennedy reasoned there could be no *private* aiding and abetting cause of action implied in the Act's language.[168] The opinion did not clearly state whether it barred government causes of action under an aiding and abetting theory, so Congress enacted the Private Securities Litigation Reform Act (PSLRA) in 1995 to provide some much needed clarity.[169] The PSLRA explicitly stated *inter alia* that the SEC is able to bring aider and abettor claims, and it has since brought several cases under this theory.[170]

For instance, in *SEC v. DiBella*, a Connecticut senator convinced the state treasurer to invest money from the state's retirement trust fund with a particular asset management firm, for which he was paid a finder's fee.[171] After the treasurer pled guilty to federal racketeering charges, the SEC brought charges against the senator for aiding and abetting the treasurer.[172] The Second Circuit upheld the senator's conviction because the SEC presented substantial evidence showing that the senator knew about the investment scheme, helped the treasurer invest in the asset management firm, and persuaded the treasurer to increase his investments in order to get a higher fee.[173] These actions amounted to aiding and abetting because the senator did not commit the fraud himself, but provided substantial assistance to the treasurer who did.[174]

Conversely, in *SEC v. Papa*, the First Circuit rejected the SEC's theory that three executives of Putnam Fiduciary Trust Company aided and abetted three other executives' scheme to defraud a client by helping them cover up their failure to timely invest the client's assets in a defined benefit plan in early 2001, costing the client $4 million.[175] The SEC alleged that the three defendants signed letters to Putnam's external auditor in 2002 and 2003 that stated they were "unaware of any uncorrected errors, frauds or illegal acts" in connection with the transaction, but the First Circuit was not persuaded because those denials, while wrongful, occurred more than a year after the

[167] *Id.* at 182.

[168] *Id.* at 184–85.

[169] Private Securities Litigation Reform Act of 1995, Pub. L. No. 104-67, § 104, 109 Stat. 737, 757 (codified as amended in scattered sections of 15 U.S.C.).

[170] 15 U.S.C. § 78t(e) (2006); *see also* S. REP. NO. 104-98, at 13 (1995) (stating that the PSLRA helped "clarify[ ] the ability of the SEC to bring aiding and abetting claims").

[171] SEC v. DiBella, 587 F.3d 553, 558–60 (2d Cir. 2009).

[172] *Id.* at 560.

[173] *Id.* at 565–67.

[174] *Id.* at 567.

[175] SEC v. Papa, 555 F.3d 31, 33–34 (1st Cir. 2009).

transaction had been completed.[176] The court said that convicting these defendants would have extended aiding and abetting liability too far, for one cannot aid and abet a fraud that has already occurred.[177]

These cases demonstrate how the courts have not let the SEC run rampant with charging nonprimary violators—or those who did not commit the actual trade but may still have liability—with aiding and abetting violations of the securities laws. The next section applies the aiding and abetting theory to the hacker-seller paradigm, and argues that charging hacker-sellers under the aiding and abetting theory does not, as feared by the *Papa* court, extend aiding and abetting liability too far.

B. Why Aiding and Abetting Liability Is a More Effective Method for Charging Hacker-Sellers with Insider Trading

The most compelling reason that the aiding and abetting theory is better suited for charging hacker-sellers with insider trading than 10b-5 is that the theory properly encapsulates the hacker-seller's conduct. The hacker-seller is better characterized as a facilitator of insider trading than as a primary culprit because it is difficult to assess the hacker's conduct as giving rise to primary insider trading liability.[178] Charging the hacker under the aiding and abetting theory appropriately treats the conduct as secondary to the primary insider trading violation that was perpetrated not by the hacker-seller, but by the actual trader.

A breakdown of circuit courts' three-pronged approach to prosecuting aiders and abettors of securities laws illuminates this idea. The primary securities violation is the actual trade the recipient of the information commits on the basis of the information the hacker-seller provides. The relationship between the hacker-seller and the trader mirrors a tipper-tippee relationship as seen in *Dirks*.[179] The hacker-seller would be the tipper who obtained the material nonpublic information and provided it to the tippee, the trader, to trade on. The tippee is the trader, who commits the primary securities violation by trading on material nonpublic information supplied by the tipper.

The hacker-seller must also have knowledge of the primary actor's—the trader's—impending securities violation.

[176] *Id.* at 34–36.

[177] *Id.* at 37.

[178] *See supra* Part II (discussing why the hacker-seller cannot be charged under the three existing theories of primary insider trading liability).

[179] *See supra* notes 43–45 and accompanying text.

The hacker-seller must be aware of the trader's intent to trade on the basis of the information supplied. It is unlikely that the hacker-seller would give the nonpublic information away without knowing what the trader plans to do with the information once acquired. This knowledge requirement is satisfied if the hacker-seller is hired to acquire information for the trader, or if the hacker conspires with the trader, because in both scenarios the hacker is still aware of the trader's intent to trade on the basis of the newly acquired information. So long as the hacker-seller knows the trader will trade on the basis of the information acquired, the knowledge requirement is satisfied. The final prong asks whether the secondary actor provided substantial assistance to the primary actor. Here, the hacker-seller provides substantial assistance to the underlying trade by acquiring the information used to commit the primary securities violation and by providing said information to the trader in advance of the transaction. Without the hacker-seller's actions, the trade cannot occur. Like the senator in *DiBella*, the hacker-seller's actions occur before the actual trade and facilitate the primary actor's, in this case, the trader's, securities violation.[180]

Although this approach still premises the hacker-seller's liability on the actions of another person, it successfully attaches liability to the hacker-seller by employing a different analysis than the affirmative misrepresentation theory. It is difficult to capture hacker-sellers under the affirmative misrepresentation theory because that theory attaches liability to the violator when the trade on the basis of material nonpublic information occurs, not when the information is wrongfully acquired.[181] Since hacker-sellers sell the information to another person—the trader—instead of trading on it themselves, their conduct is therefore not "in connection with" a securities transaction under the Exchange Act.[182] The aiding and abetting theory targets this exact kind of culprit, one who does not commit the primary violation (in this case, securities fraud), but through whose conduct another person can. While the tangential relationship between the hacker-seller and the trader is the undoing of the affirmative misrepresentation theory, it is the lynchpin of the aiding and abetting theory.

More importantly, the language of Section 20(e) allows the hacker-seller to be charged with the primary offense, too.

[180] SEC v. DiBella, 587 F.3d 553, 567 (2d Cir. 2009).

[181] *See supra* Section II.C.

[182] *See supra* Section II.C.

18 U.S.C. Section 2(a) reads, "[w]hoever commits an offense against the United States or *aids, abets,* counsels, commands, induces or procures its commission, is punishable as a principal."[183] Section 20(e) of the Securities Exchange Act adopts this language for securities violations, allowing for those convicted of aiding and abetting a violation of the securities laws to be liable for the actual violation too.[184] In the case of the hacker-seller, this means that if he is charged with aiding and abetting the trader's securities violation, then he can be held liable for that violation too.

C. Policy Considerations Supporting the Aiding and Abetting Theory

The aiding and abetting theory gives the SEC the ability to prosecute hacker-sellers under the securities laws. While it is possible to prosecute them under different federal statutes too, the securities laws should not be left out because they are a much stronger deterrent against their criminal conduct and charging hacker-sellers under the securities laws comports with public policy considerations that have supported the securities laws since their inception.

1. Securities Laws Impose Stricter Penalties than the Alternatives

Hacker-sellers actually commit crimes that are covered by three different criminal support statutes: the Computer Fraud and Abuse Act (CFAA) prohibits the hacking itself,[185] and the Mail Fraud and Wire Fraud Statutes proscribe the subsequent sale of the material nonpublic information.[186] All three statutes carry similar sentences: defendants convicted under them can be fined up to $1 million, imprisoned up to twenty years,[187] or both.[188]

[183] 18 U.S.C. § 2(a) (2012) (emphasis added).

[184] 15 U.S.C. § 78t(e) (2012).

[185] 18 U.S.C. § 1030(a)–(c). The CFAA prohibits "intentionally access[ing] a [protected] computer without authorization" and obtaining "information contained in a financial record [belonging to] a financial institution." *Id.* § 1030(a)(2)(A). "[P]rotected computer" is defined under § 1030(e)(2) to mean a computer exclusively used by a financial institution or one that "is used in or affecting interstate or foreign commerce." *Id.* § 1030(e)(2).

[186] *See* 18 U.S.C. §§ 1341, 1343. The Mail Fraud Statute and Wire Fraud Statute prohibit fraudulent schemes to deprive others of money or property using the mails or wires in furtherance of that scheme. *Id.*

[187] *See* Nate Raymond, *Insider Traders in U.S. Face Longer Prison Terms, Reuters Analysis Shows*, REUTERS (Sept. 2, 2014), http://www.reuters.com/article/us-insidertrading-prison-insight-idUSKBN0GX0A820140902 [https://perma.cc/VXK6-RKUP].

[188] 18 U.S.C. §§ 1030, 1341, 1343. The Sarbanes-Oxley Act of 2002 increased the maximum prison term from five years to twenty. The Sarbanes-Oxley Act of 2002,

The length of imprisonment largely correlates with the amount of trading gains, but the average sentence is usually very short. From 2008 to 2013, insider trading defendants were sentenced for an average of 17.3 months of jail time.[189]

The Securities Act provides the SEC with a far more potent arsenal with which it can penalize hacker-sellers in addition to the sentences available under the fraud statutes, including injunctive relief, asset freezing, and civil penalties up to three times the illegal profits made or the losses avoided from the securities violation.[190] However, the two strongest deterrents available to the SEC are disgorgement and repatriating profits made by foreign defendants. Disgorgement dissuades securities violations by depriving perpetrators of profits obtained through securities violations and prevents their unjust enrichment.[191] The SEC has entered into numerous agreements with foreign countries allowing the pursuit of international violators of American securities laws.[192] This ability is crucial to the case of hacker-sellers because they will still be within the SEC's grasp if they sell the information to foreign traders who use it to trade on American securities. The CFAA, Mail Fraud Statute, and Wire Fraud Statute do not provide such capabilities.[193]

2. Flexibility of the Securities Laws

Section 10(b) and Rule 10b-5 were construed very broadly with the goal of "encompass[ing] the infinite variety of devices by which undue advantage may be taken of investors and others."[194] The Supreme Court has espoused this sentiment several times

Pub. L. No. 107-204, § 903(a)–(b), 116 Stat. 745, 805 (codified as amended at 18 U.S.C. §§ 1341, 1343 (2012)).

[189] Raymond, *supra* note 187.

[190] 15 U.S.C. §§ 78u(d)(1), 78u-1, 78u-2 (2012); *see also* WILLIAM K.S. WANG & MARC I. STEINBERG, INSIDER TRADING 639–41 (3d ed. 2010); *Securities Fraud*, 52 AM. CRIM. L. REV. 1567, 1625–37 (2015); *see supra* Section II.C.

[191] *See* SEC v. Cavanagh, 445 F.3d 105, 117 (2d Cir. 2006) ("In a securities enforcement action . . . 'disgorgement' is not available primarily to compensate victims. Instead, disgorgement has been used . . . to prevent wrongdoers from unjustly enriching themselves through violations, which has the effect of deterring subsequent fraud." (footnote omitted)); SEC v. Warde, 151 F.3d 42, 50 (2d Cir. 1998) (describing the proper level of disgorgement as "the difference between the price of . . . [the stock] when purchased on inside information and [its] price after the disclosure of the inside information"); Tex. Am. Oil Corp. v. U.S. Dep't of Energy, 44 F.3d 1557, 1570 (Fed. Cir. 1995) ("When those injured are not restored to their previous position the disgorgement partakes not of restitution, but of recovery by government of the illegal gains for remedial and enforcement purposes.").

[192] *Securities Fraud*, *supra* note 190, at 1633–35 (explaining the various agreements the SEC has entered into with foreign countries or organizations that allow it to conduct international investigations and discussing Congressional legislation that enables the SEC to take action based on foreign convictions).

[193] *See* 18 U.S.C. §§ 1030, 1341, 1343.

[194] *In re* Cady, Roberts & Co., No. 8-3925, 40 SEC Docket 907, 911 (Nov. 8, 1961).

over the decades, saying that it must interpret the securities laws "not technically and restrictively, but flexibly to effectuate its remedial purposes."[195] Furthermore, and perhaps more appropriately, Congress has pointed out that the securities laws should adapt to changing "technological conditions."[196]

This adaptability allows the securities laws to be applied to several different types of conduct. It is unlikely that when Congress promulgated the Securities Exchange Act,[197] it envisioned computer hacking as a method by which insider trading could occur.[198] The first known instance of computer hacking occurred in 1980, well after the Securities Exchange Act was enacted.[199] Therefore, hacking cannot be captured by the securities laws if the laws are interpreted strictly, but it would be captured by the more flexible interpretation that Congress has suggested.[200]

3. Economic Unfairness

One goal of 10b-5, and the securities laws as a whole, is to protect the integrity of the markets from abuse by those who use nonpublic information for advantageous trades.[201] The "integrity of the markets" rationale is grounded in the notion that the price of shares as they are traded on the markets reflects all publicly available information.[202] As one court put it, "it is hard to imagine that there ever is a buyer or seller who does not rely on market integrity. Who would knowingly roll the dice in a crooked crap game?"[203] The hacker-seller's actions fly in the face of this central tenet of 10b-5 because they facilitate trading based on nonpublic information. The outsider would then buy or sell at an inaccurate price because he cannot take into account the change in the price as a result of the illicit trade, thereby being deprived of the full gain he would have obtained had he traded on the security's true value. Not only would this

[195] SEC v. Zandford, 535 U.S. 813, 819 (2002) (quoting SEC v. Capital Gains Research Bureau, Inc., 375 U.S. 180, 186 (1963)); *see, e.g.*, Chadbourne & Parke LLP v. Troice, 134 S. Ct. 1058 (2014); Ernst & Ernst v. Hochfelder, 425 U.S. 185, 202–04, 206 (1976); Affiliated Ute Citizens v. United States, 406 U.S. 128, 151 (1972).

[196] H.R. REP. NO. 94-29, at 92 (1975).

[197] The 73rd Congress promulgated the Securities Exchange Act in 1934. Securities Exchange Act of 1934, Pub. L. No. 73-291, 48 Stat. 881 (codified at 15 U.S.C. §§ 78a–qq (2012)).

[198] *See* SEC v. Dorozhko, 574 F.3d 42, 49 (2d Cir. 2009).

[199] 3 JAMES W. CORTADA, THE DIGITAL HAND: HOW COMPUTERS CHANGED THE WORK OF AMERICAN PUBLIC SECTOR INDUSTRIES 135 (2008).

[200] *See supra* note 196 and accompanying text.

[201] 77 CONG. REC. 2301, 2934 (1933) (remarks of Rep. Chapman).

[202] Basic Inc. v. Levinson, 485 U.S. 224, 246 (1988).

[203] *Id.* at 246–47 (quoting Schlanger v. Four-Phase Sys. Inc., 555 F. Supp. 535, 538 (S.D.N.Y. 1982)).

be fundamentally unfair, but it would create an inefficient market to the outsider who would be deprived of the opportunity to buy or sell at the right price.[204] While the blanket characterization of insider trading as unfair has been challenged on the grounds that it can create a more efficient market,[205] this argument applies only when the information that was traded on is obtained legally. The argument that insider trading can sometimes create a more efficient market does not apply to illegal insider trading, and the hacker-seller certainly acquires the information they sell via illegal means.[206]

CONCLUSION

Hacker-sellers present a new type of insider trading culprit whose liability under 10b-5 remains outside the scope of the classical, misappropriation, and affirmative misrepresentation theories. This note suggests that they should be charged instead under Section 20(e) with aiding and abetting the securities violation perpetrated by the recipient of the material nonpublic information. It is more appropriate to charge them this way because their conduct will be properly characterized as facilitating the primary securities violation while simultaneously imbuing liability for the underlying violation.

Charging hacker-sellers this way is supported by the underlying policy considerations of the securities laws and ensures that hacker-sellers will be subject to stronger penalties than those available under other federal laws. The SEC can prosecute this new breed of insider trader, but it should do so under the aider and abettor theory codified in Section 20(e) instead of 10b-5.

Ryan H. Gilinson[†]

[204] Chiarella v. United States, 455 U.S. 222, 241 (Burger, C.J., dissenting).

[205] HENRY G. MANNE, INSIDER TRADING AND THE STOCK MARKET 77–91 (1966) (Insider trading allows the market price of securities to reflect the value of the inside information because the trades on the basis of that information would occur before the security goes public. The securities would then be traded on the public markets after the inside trades have occurred, and at that point they would be trading at their proper price.).

[206] *See supra* Section IV.C.1 (discussing the other federal laws the hacker-seller violates in his acquisition of material nonpublic information).

[†] J.D. Candidate, Brooklyn Law School, 2017; B.A., University of Florida, 2014. I would first like to thank Jessica Schneider, Valentina Lumaj, Zack Goldberg, Jacey Gottlieb, Lillian Smith, Michael Piacentini, Myra Din, Nick DeLisa, and the whole *Brooklyn Law Review* for all of their help in preparing this note for publication. I would also like to thank my family and friends for their unwavering support throughout the process of writing this note. Finally, I would like to thank my parents and my brother for their endless love and support, and for inculcating a passion for reading and writing in me, without which this note could not have been written.