Journal of International Business and Law

Volume 15 | Issue 2 Article 7

3-1-2016

Circumventing Insider Trading Laws by Cyberhacking: A Look into the Vulnerability of Cybersecurity Breaches in Regards to Insider Trading

Sonal Sahel

CIRCUMVENTING INSIDER TRADING LAWS BY CYBERHACKING: A LOOK INTO THE VULNERABILITY OF CYBERSECURITY BREACHES IN REGARD TO INSIDER TRADING

by Sonal Sahel

I. INTRODUCTION

In April 2014, there was a large online security breach known as the 'heartbleed bug,' which compromised private and confidential information for many large and well-known companies.[1] There have been news reports in which experts state that these breaches go beyond the surface of people's passwords, social security numbers and other confidential information being leaked.[2] These experts state that illegal insider trading may have occurred since many public companies that were affected by the security bug saw a drop in their stocks prior to the release of unwelcoming news, such as letting the public know that their systems had been hacked.[3] The evidence of stock prices falling prior to the public release of the negative news, may indicate that the security breach led to the release of private and confidential information, which in turn led to investors selling their stocks before the news release and its immediate stock price drop.[4] In today's society, information travels rapidly due to the advanced technology we are now accustomed to, which accentuates the stock market's fluctuations.[5]

Technology has changed many aspects of business that were traditionally kept in paper format into a digital form, including secured databases on the Internet. Companies are keeping information about their clients, such as passwords, social security numbers and other private data online. On the other hand, consumers are willingly giving the information to companies online, with the understanding that it is through a secured network.[6] In addition, companies keep various internal documents online due to the ease of organization and ability to work efficiently in our modern and global society.[7] Examples of these internal documents include financial data, stock information, private timelines for releasing information publically, etc.[8]

---

[1] Ryan Sherwin, *Heartbleed bug may have caused insider trading, says web security expert*, THE INDEPENDENT (Apr. 30, 2014), http://www.independent.co.uk/life-style/gadgets-and-tech/news/heartbleed-bug-may-have-caused-insider-trading-says-web-security-expert-9307848.html.

[2] Gerry Smith, *Your Favorite Websites Could Have Warned You About Heartbleed, But Didn't*, HUFFINGTON POST (Apr. 17, 2014), http://www.huffingtonpost.com/2014/04/17/websites-heartbleed_n_5161298.html.

[3] Sherwin, *supra* note 1.

[4] *Id.*

[5] Tamar Frankel, *The Internet, Securities Regulation, and Theory of Law*, 73 CHI.-KENT L. REV. 1319, 1334 (1998).

[6] Lauren C. Williams, *The Heartbleed Bug Reveals We're Willing To Give Up Online Security To Feel More Connected*, THINK PROGRESS (Apr. 12, 2014), http://thinkprogress.org/culture/2014/04/11/3425310/what-the-heartbleed-bug-says-about-our-interconnectivity.

[7] *Id.*

[8] FTC, COPIER DATA SECURITY: A GUIDE FOR BUSINESSES (Nov. 2010).

The fear of insider trading resulting from the heartbleed bug forces us to turn to the regulations to determine if such transactions are illegal and chargeable. The Securities Exchange Act was enacted in 1934,[9] a time when the technology and wealth of information that we have today was unimaginable. Due to the various enhancements that the Internet and other technology bring, many companies keep a great deal of information online.[10] There are great advantages of utilizing the Internet's ability, such as having nearly immediate access from all corners of the world and sharing information with specific parties easily. Staying organized in an efficient and cost effective manner are further benefits of the Internet, compared to boxes and cabinets of files. The unfortunate consequence of online storage is that it leaves this information vulnerable to getting into the wrong hands via security breaches/hackers.

Companies and consumers have been using technology in this manner for decades and it has gained a place in society with the assumption that this information is private and secured.[11] Recent security breaches through Internet bugs such as the April 2014 'heartbleed' bug and the September 2014 'shellshock' bug,[12] have brought a quick and a delayed realization that not all information is secure.[13] These Internet bugs are infiltrating the database and servers of various public companies, leading to privacy and identification violations. Information such as names, social security numbers and addresses may be getting in the wrong hands, creating the possibility of insider trading transactions.[14]

Despite society's dependency on the Internet, there are currently no cybersecurity requirements placed on private companies.[15] The lack of cybersecurity requirements poses a number of dangers, potentially including insider trading transactions.[16] Society's current failure to enact cybersecurity standards makes hackers capable of obtaining private information that they are not privy too.[17] Furthermore, the information that hackers have the ability to obtain can be circulated to others who cannot be subject to insider trading actions due to the current interpretation of the laws.[18]

Internet security breaches are unique in that they are extremely to track and therefore often get away with crimes and leave havoc in their path.[19] Security breaches have presented a great number of issues; such as identify theft, email and other communication

---

[9] 15 U.S.C. § 78j(b) (2012).

[10] Through various 'online' platforms, such as clouds, emails, servers, etc.

[11] *Consumers of All Ages More Concerned About Online Data Privacy*, EMARKETER (May 6, 2014), http://www.emarketer.com/Article/Consumers-of-All-Ages-More-Concerned-About-Online-Data-Privacy/1010815#sthash.z1wBs6GC.dpuf.

[12] David Gilbert, *Shellshock: What Cyber Security Experts Have to Say About Bash Bug*, IB TIMES (Sept. 26, 2014), https://uk.news.yahoo.com/shellshock-cyber-security-experts-bash-bug-101828223.html#wRqZsVv.

[13] Sam Frizell, *Report: Devastating Heartbleed Flaw Was Used in Hospital Hack*, TIME MAG. (Aug. 20, 2014), http://time.com/3148773/report-devastating-heartbleed-flaw-was-used-in-hospital-hack.

[14] Sherwin, *supra* note 1.

[15] ERIC A. FISCHER, CONG. RESEARCH SERV., R42114, FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW AND DISCUSSION OF PROPOSED REVISIONS 1-2 (2013).

[16] Sherwin, *supra* note 1.

[17] *Id.*

[18] SEC v. Dorozhko, 574 F.3d 42 (2d Cir. 2009).

[19] Elizabeth Orton & Chris Schlag, *Creating a Model of Cyber Proficiency: Remodeling Law Enforcement Tactics in Pittsburgh to Address the Evolving Nature of Cybersecurity*, 14 PGH. J. TECH. L. & POL'Y 276, 278 (Spring 2014).

privacy violations, and the virtual impersonation of others.[20] This Note will deal exclusively with the insider trading issue that Internet security breaches have presented.[21]

As companies have a great desire to keep information online, laws to protect this information are also necessary. There is a serious concern regarding the ability of cyberhackers[22] to steal corporate information and evade insider trading regulations. Since a cyberhacker is not a corporate insider,[23] they have no fiduciary duty to the company and therefore cannot satisfy the elements of insider trading and neither can those who they pass the hacked information to, known as tippees.[24]

Part II of this Note will present the current securities laws regarding insider trading, how they are being interpreted and applied, and why they no longer protect all aspects of potential insider trading. Part III analyzes how the current laws are being circumvented and Part IV identifies how both the insider trading regulations need to be amended to account for hackers and that cybersecurity regulations must be implemented.

II. CURRENT INSIDER TRADING MATTERS

Today's Insider Trading Laws

The Securities Exchange Commission ("SEC") states that it prohibits insider trading "[b]ecause insider trading undermines investor confidence in the fairness and integrity of the securities markets."[25] Enforcing the insider trading regulations aims to ensure that people are not wrongfully profiting off of companies, due to their position of having private and confidential material information,[26] prior to the general public and relying on that information for their personal gain.[27] Insider trading is a large issue evidenced by studies stating that insiders make $5 billion dollars each year due to trading on private information.[28] Securities fraud is a sizeable concern for public companies, and those who are profiting can only be

---

[20] The Heartbleed Bug, CODENOMICON, http://heartbleed.com (last updated Apr. 29, 2014).

[21] Chris Green, *Shellshock superbug: Can anything stop the hackers? Millions of users' online details at risk*, THE INDEPENDENT (Sept. 26, 2014), http://www.independent.co.uk/life-style/gadgets-and-tech/news/shellshock-criminals-may-already-be-exploiting-biggest-ever-computer-bug-9758146.html.

[22] The definition of cyberhack comes from the combination of cyber and hack. Cyber is defined as "of, relating to, or involving computers or computer networks (as the Internet)." Cyber – definition, Merriam-Webster Dictionary, MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary/cyber (last visited Feb 1., 2015). Hack is defined as "to gain access to a computer illegally." Hack – definition, Merriam-Webster Dictionary, MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary/hack (last visited Feb. 1, 2015).

[23] Corporate insiders are defined as officers, directors, and 10% shareholders. (Ernst & Ernst v. Hochfelder, 425 U.S. 185, 209, n. 28 (1976).

[24] Tippees are defined as those who receive material nonpublic information from tippers and can be liable for trading on the information. Dirks v. SEC, 463 U.S. 646, 647 (1983).

[25] *Insider Trading*, SEC, http://www.sec.gov/answers/insider.htm (last visited Jan. 30, 2015).

[26] Material information is defined by the Supreme Court as information in which 'there is a substantial likelihood that a reasonable shareholder would consider it important in deciding how to [trade]." TSC Industries, Inc. v. Northway, Inc., 426 U.S. 438, 439 (1976).

[27] *Insider Trading, supra* note 25.

[28] Jesse M. Fried, *Reducing the Profitability of Corporate Insider Trading Through PreTrading Disclosure*, 71 S. CAL. L. REV. 303, 306 (1998).

found guilty if there is the intent to defraud through manipulation or deception.[29] Security breaches on the Internet may allow hackers to steal material nonpublic information and pass it on to others.

A tipper is the one that owes a fiduciary duty to the company and breaches their duty by passing material nonpublic information on to a tippee with the requisite scienter.[30] Scienter is the intent to commit fraud or reckless disregard for the truth, which goes beyond mere negligence.[31] Scienter on the part of the tipper means deliberately or recklessly passing on confidential information to a tippee when the tippee is aware that the tipper is breaching their fiduciary duty.[32]

Tippees are those who receive material nonpublic information from tippers and can be liable for trading on the information.[33] The requisite scienter of the tippee is when the tippee knows that the information that they have received is material nonpublic information, and the tippee knows or should know that the information would be in breach of the tipper's fiduciary duty.[34]

Fiduciary duty is the duty owed by those who have access to nonpublic information, to act in the best interest of the company.[35] A fiduciary duty further requires those who hold material nonpublic information to abstain from relying on the information or to disclose the information publically.[36] Per case precedent,[37] a tippee can be charged with insider trading if it can be shown that the identifiable tipper has breaching their fiduciary duty.[38]

The illegality of insider trader is found in section 10(b) of the Securities Exchange Act of 1934.[39] Section 10(b) prohibits "any manipulative or deceptive device or contrivance" in connection with "the purchase or sale of any security."[40] In 1934, Congress created the SEC to enforce the Securities Exchange Act.[41] Through the powers given to the SEC to regulate the securities markets, the SEC codified insider trading rules as rule 10b-5.[42]

Rule 10b-5 forbids any person "[t]o employ any device, scheme, or artifice to defraud" and "[t]o 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" on the securities markets.[43] Rule 10b-5-1 holds that "the purchase or sale of a security of any issuer, on the basis of material nonpublic information ... in breach of a duty of

---

[29] Dirks v. SEC, 463 U.S. 646, 663, n. 23 (1983); 15 U.S.C. § 78j(b) (2012).

[30] *Dirks*, 463 U.S. at 663, n. 23.

[31] Ernst & Ernst v. Hochfelder, 425 U.S. 185, 193, n.12 (1976); SEC v. McNulty, 137 F.3d 732, 741 (2d Cir. 1998).

[32] *Dirks*, 463 U.S. at 660-62.

[33] *Id.* at 660.

[34] *Id.*

[35] Hagar Cohen, *Cracking Hacking: Expanding Insider Trading Liability in the Digital Age*, 17 SW. J. INT'L L. 259, 274 (2011).

[36] *Dirks*, 463 U.S. at 647.

[37] *See id.*

[38] *Id.*

[39] 15 U.S.C. § 78j(b) (2012).

[40] *Id.*

[41] The Investor's Advocate: How the SEC Protects Investors, Maintains Market Integrity, and Facilitates Capital Formation, SEC, http://www.sec.gov/about/whatwedo.shtml#create (last modified June 13, 2013).

[42] 17 C.F.R. § 240.10b-5 (2012).

[43] § 240.10b-5(a), (c) (2012).

trust or confidence that is owed ... to the [company] ... or to any other person who is the source of the material nonpublic information.[44] Furthermore, rule 10b-5-2 prohibits "the purchase or sale of securities on the basis of, or the communication of, material nonpublic information misappropriated in breach of a duty of trust or confidence."[45]

Insider trading is an activity that the SEC would greatly like to avoid, and thus the Regulation Fair Disclosure ("Regulation FD") requirement was adopted in October of 2000 to further deter and identify potential insider trading action.[46] Regulation FD requires all public companies to file a Form 8-K and disclose material nonpublic information, thus making it public, when an insider discloses material nonpublic information to enumerated persons.[47] This regulation was passed to preclude selective disclosure by public companies and allow everyone to gain access to the same information at the same time.[48]

Intentional selective disclosure requires the company to file the Form 8-K simultaneously with the selective disclosure, thus ensuring that those in the selective disclosure group are unable to trade on the newly public information prior to the information circulating and having the ability to profit like insider trading offenders.[49] For unintentional selective disclosure, the public disclosure must be made promptly.[50] Regulation FD was implemented to encompass those who evaded Rule 10b-5 violations by stating that the information was public at the time that they relied and traded on the information. In reality, these evaders happened to gain information before it had a chance to circulate through publically, thus allowing sufficient time to conduct trades prior to the markets accounting for and adjusting to the newly publicized information.[51] Therefore, such traders were profiting from the markets by an arrangement similar to insider trading transactions.[52]

Insider trading is broken up into two theories: the classical theory and the misappropriation theory.[53] Under the classical theory, those considered insiders are liable to the company as they have a fiduciary duty to the company; those insiders have been defined as officers, directors and 10% shareholders.[54] Secondly, the misappropriation theory broadly applies when securities are traded with reliance on material nonpublic information in breach of the fiduciary duty owed to the company.[55]

Under the misappropriation theory, the seminal case is *SEC v. O'Hagan*.[56] *O'Hagan* demonstrates how insider trading actions have expanded beyond the classical theory. O'Hagan, an attorney of a law firm, was guilty of insider trading by relying and trading on

---

[44] § 240.10b5-1. SEC codifies that awareness is enough. *Id.*

[45] § 240.10b5-2. SEC ensures that they are able to count family members as tippees. *Id.*

[46] Selective Disclosure and Insider Trading, 17 C.F.R. § 240, 243, 249 (2000) available at http://www.sec.gov/rules/final/33-7881.htm (Aug. 15, 2000).

[47] *Id.*

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] *Id.*

[53] Allan Horwich, *The Origin, Application, Validity, and Potential Misuse of Rule 10b5-1*, 62 THE BUS. LAW., 914, 916 (May 2007).

[54] Matter of Cady, Roberts & Co., Release No. 6668, Release No. 34-6668, 40 SEC 907, 3 (Nov. 8, 1961).

[55] United States v. O'Hagan, 521 U.S. 642, 652 (1997).

[56] *O'Hagan*, 521 U.S.

material nonpublic information of the law firm's client, a public company.[57] The Court found that O'Hagan violated section 10(b) as the deceptive device used for the purchase of stock was the reliance of material nonpublic information obtained through his position.[58] The defendant obtained the material nonpublic information in confidence, which also gave rise to a fiduciary duty to the company.[59] O'Hagan was convicted of insider trading, despite not being an insider, [60] thus also establishing that an outsider can be a tippee within the 'Dirks test.'[61]

The Dirks test was established by *Dirks v. SEC*[62] and is used to determine if a tippee is liable for insider trading. *Dirks* expanded insider trading regulations by finding that the misappropriation theory can extend to third parties (tippees).[63] The Dirks test is satisfied when a tipper breaches their fiduciary duty to the company by passing material nonpublic information to the tippee, along with their fiduciary duty to abstain or disclose to a tippee.[64] A tipper has breached their fiduciary duty to the company if they passed the material nonpublic information on with scienter and in exchange of a personal benefit.[65]

Under the Dirks test, it should be noted that a tippee can pass the information on to another tippee, known as a remote tippee and continue the chain of liability.[66] Remote tippees are liable if they trade on information that they know, or have reason to know, derives from a breach of fiduciary duty.[67] Remote tippees have also been liable when they stated that they did not want to know the source of the information.[68] Further, the first tippee must pass the information on intentionally or recklessly to the remote tippee(s) for their own benefit and have or should have knowledge that the information was obtained through a breach of fiduciary duty.[69]

Given the elements of insider trading liability, a tippee is only liable if they know or have reason to know that the tipper is breaching their fiduciary duty, as the tippee's duty is derived from the tipper's duty.[70] In December 2014, the Second Circuit recently added to the SEC's burden, by finding that a tippee is only liable under insider trading laws if they had *actual knowledge* that the tipper gained a personal benefit and breached their fiduciary duty which was passed onto the tippee.[71]

---

[57] *Id.* at 659.

[58] *Id.* at 643.

[59] *Id.*

[60] *Id.* at 666.

[61] *Id.*; *see* Dirks v. SEC, 463 U.S. 646, 653-58 (1983).

[62] 463 U.S. 646 (1983).

[63] *See* Donald C. Langevoort, *"Fine Distinctions" in the Contemporary Law of Insider Trading*, 2013 COLUM. BUS. L. REV. 429, 451 (2013).

[64] Chiarella v. United States, 445 U.S. 222, 226-27 (1980).

[65] 463 U.S. 646, 647, 663 (1983).

[66] United State v. Falcone, 257 F.3d 226, 227 (2d Cir. 2001); United States v. McDermott, 245 F.3d 133, 135-36 (2d Cir. 2001); SEC v. Musella, 678 F. Supp. 1060, 1063 (S.D.N.Y. 1988); Dirks v. SEC, 463 U.S. 646, 649-50 (1983).

[67] *See* SEC v. Musella, 678 F. Supp. 1060, 1063 (S.D.N.Y. 1988).

[68] *Id.*

[69] *Id.*

[70] *Dirks*, 463 U.S. at 647.

[71] United States v. Newman, 773 F.3d 438, 449 (2d Cir. 2014).

A third type of insider trading that has been adopted is Rule 14e-3, [72] after the judicial determination of *Chiarella v. United States*.[73] In *Chiarella*, the defendant escaped SEC insider trading rules as the Court found that Chiarella derived no fiduciary duty from anyone when inadvertently gained material nonpublic information regarding a tender offer.[74] Without being under the jurisdiction of Rule 10b-5, Chiarella had no obligation to abstain or disclose prior to relying on the information.[75] To counteract the holding from *Chiarella*, the SEC adopted Rule 14e-3 which prohibits any person with material nonpublic information regarding a tender offer to disclose the information to the public or to trade in securities that are connected with the tender offer.[76]

To clarify, a tippee cannot be held liable for insider trading without the tipper breaching their fiduciary duty and gaining a personal benefit from passing the material nonpublic information.[77] This paper deals with the misappropriation theory, as security breaches and the tippees who trade on that information are generally not an officer, director or 10% shareholder of the company.[78]

Application of Current Insider Trading Laws

The SEC has stated in recent years that it would like to make insider trading actions a high priority, to ensure integrity of the markets.[79] In 2013, the SEC brought 44 insider trading enforcement actions and 52 actions in 2014.[80] Despite the clear intent of the SEC, the current laws do not explicitly consider the new realm of technology and its position in the world of insider trading. The SEC did have a positive breakthrough regarding insider trading and cyberhacking in the Second Circuit, with the case of *SEC v. Dorozhko*,[81] which is discussed at length below.

Can we define the Internet security breaches and hackers as tippers? If not, there is no fiduciary duty owed, thus allowing tippees who are passed material nonpublic information from tippers to profit, as they are not restricted by a duty to the company to abstain or disclose the information.[82] If yes, then how do these hacker tippers hold a fiduciary duty to the company regarding their material nonpublic information and can the hackers be identified? This is the issue that society is currently presented with. Those who possess material nonpublic information without a fiduciary duty to the company to abstain or disclose is free to rely and trade on the information.[83]

---

[72] 17 CFR § 240.14e-3 (2012).

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

[74] *Id.*

[75] *Id.* at 227.

[76] 17 CFR § 240.14e-3 (2012).

[77] Dirks v. SEC, 463 U.S. 646, 647, 654 (1983).

[78] Matter of Cady, Roberts & Co., 40 SEC 907, 4 (Nov. 8, 1961).

[79] *SEC Continues Aggressive Insider Trading Enforcement*, WECOMPLY (May 15, 2014), http://www.wecomply.com/post/2220481-sec-continues-aggressive-insider-trading-enforcement.

[80] Year-by-Year SEC Enforcement Statistics, SEC, https://www.sec.gov/news/newsroom/images/enfstats.pdf (last visited Feb. 1, 2015).

[81] 574 F.3d 42 (2d Cir. 2009).

[82] *Id.* at 45.

[83] Dirks v. SEC, 463 U.S. 646, 660 (1983).

Due to the narrow requirements of tippers, the security breaches are unable to satisfy the requirements of a tipper. Though it is arguable that tippees of information obtained through security breaches are identifiable, tippees can only be charged if the tipper breached a fiduciary duty by disclosing information to the tippee and if the tippee knows or has a reason to know of the breach.[84] Furthermore, tippees must have knowledge of a fiduciary duty, which is breached with manipulation or deception, which is not possible as there is no identifiable tipper who has a fiduciary duty.[85] Therefore, there is currently no duty for a tippee to abstain or disclose the nonpublic information simply by holding the said information.[86]

Though insider trading laws have been around for 80 years, dealing with the new technologies aspect has been difficult. Challenges are furthered by the fact that there are currently no cybersecurity laws that carry substantial weight and require the private sector to update their security regularly.[87] The private sector is only motivated to update their security up to the extent for which their clients and investors push. With issues such as the recent security breach bugs, cybersecurity needs to be regulated for preventative measures.

The glimmer of recognition of this issue is evident by the Second Circuit's ruling in *SEC v. Dorozhko* in 2009.[88] In this matter, the defendant hacked into the servers of Thomson Financial, who provided investor relations and had a copy of the earnings report prior to publication for publically traded company IMS Health, Inc. ("IMS").[89] The defendant was able to retrieve a copy of the earnings report and used his Interactive Brokers account for the first time to purchase put options of IMS worth $41,670.90 around 3:00pm on the same day. The defendant's purchase was one that the SEC analyzed to be extremely risky without the knowledge of the earnings projections being over 25% higher than reality.[90] The defendant's purchase accounted for 90% of the put options sold within the past six weeks.

Around 4:30pm, IMS reported the unexpected low earnings publically and saw their stock price fall 28% before the market closed for the day. The following day, within the first six minutes of the stock market opening, the defendant sold all of his IMS options, netting a profit of $286,456.59.[91] Interactive Brokers, who in turn reported the oddity to the SEC, noted the abnormality of purchase and sale.[92]

The SEC obtained a temporary restraining order to freeze the profit from the stock option sell prior to its transfer to the defendant's account in the District Court for the Southern District of New York. The District Court denied a preliminary injunction, after a preliminary injunction hearing on the basis that the SEC failed to prove a likelihood of success.[93] The District Court rationalized that computer hacking is not deceptive; since the hacker did not have a relationship of confidence[94] with the company, there was no fiduciary duty owed.[95]

---

[84] Chiarella v. United States, 445 U.S. 222, 230, n. 12 (1980).

[85] *Dirks*, 463 U.S. at 660.

[86] *Chiarella*, 445 U.S. at 223.

[87] FISCHER, *supra* note 15, at 1-2.

[88] SEC v. Dorozhko, 574 F.3d 42 (2d Cir. 2009).

[89] *Id.* at 44.

[90] *Id.*

[91] *Id.*

[92] *Id.*

[93] *Id.*

[94] *Id.* at 47, *see also* Chiarella v. United States, 445 U.S. 222, 228 (1980).

The District Court additionally emphasized to the SEC that such a threat was predictable and consciously chose to avoid addressing the issue, thus leading them down to the denial of this injunction.[96]

The SEC appealed to the Second Circuit by arguing that the defendant misrepresented himself, which is deceptive fraud and therefore within insider trading laws.[97] The Second Circuit distinguished this case from precedent, such as *Chiarella*,[98] where silence of a party was in question, as here there was an affirmative misrepresentation, which is "a distinct species of fraud."[99] The Court found that the defendant was subject to insider trading charges since misrepresentation to gain nonpublic material information is a form of fraud, but without finding a fiduciary duty.[100]

Federal administrations for the past fifteen years have placed cybersecurity as an important issue, though minimal improvements have been made.[101] The federal cybersecurity regulations, such as the Federal Information Security Management Act of 2002 ("FISMA"), only apply to government agencies.[102] Under FISMA, government agencies are required to ensure that their systems are secure by conducting periodic assessments and testing, procedures based on risk assessment, training for personnel, remedial actions to address any deficiencies and methods to detect, report and respond to security incidents.[103]

The Cyber Intelligence Sharing and Protection Act of 2012 Bill ("2012 Cyber Act Bill") passed through the House but failed to pass through the Senate.[104] The 2012 Cyber Act Bill was intended to amend the National Security Act of 1947 and give the federal government the right to information gathered by the private entities.[105] Furthermore, the bill stated that the federal government would use the cyber information gathered to confirm adequate cybersecurity to safeguard the system, and ensure confidentiality, to investigate cybersecurity crimes and to protect U.S. national homeland security.[106]

President Obama has been trying to push a cybersecurity bill through Congress in the past few years, but unfortunately with no avail.[107] As Congress has failed to assist the President with his cybersecurity agenda, President Obama signed an Executive Order to Improve Critical Infrastructure of Cybersecurity ("Executive Order") in February of 2013.[108] One of the main aims of the Executive Order was to establish specific cybersecurity

---

[95] *Dorozkho*, 574 F.3d at 45.

[96] SEC v. Dorozhko, 606 F. Supp. 2d 321, 341-43 (S.D.N.Y. 2008) *vacated*, 574 F.3d 42 (2d Cir. 2009).

[97] *Dorozkho*, 574 F.3d at 45.

[98] *See generally Chiarella*, 445 U.S. 222.

[99] *Dorozkho*, 574 F.3d at 49.

[100] *Id.* at 49-50.

[101] Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1017 (2014).

[102] 44 U.S.C. § 3541 (2012).

[103] Detailed Overview of FISMA, *NIST – Computer Security Division*, NIST.GOV (last updated on Apr. 1, 2014), http://csrc.nist.gov/groups/SMA/fisma/overview.html.

[104] *Zeichner on Presidential Action on Cybersecurity*, 2013 Emerging Issues 6932, (Lexis).

[105] H.R. 3523, 112th Cong. (2012), https://www.congress.gov/bill/112th-congress/house-bill/3523.

[106] *Id.*

[107] Michael D. Shear, *Obama to Announce Cybersecurity Plans in State of the Union Preview*, NYTIMES.COM (Jan. 10, 2015), http://www.nytimes.com/2015/01/11/us/politics/obama-to-announce-cybersecurity-plans-in-state-of-the-union-preview.html?_r=0.

[108] Zeichner, *supra* note 104; Ronald D. Lee & Nicholas L. Townsend, *Gov't Cybersecurity Standards Could Impact Many Companies*, LAW360 (Aug. 16, 2013).

requirements and standards.[109] The Order further states how issues may be addressed and increases the cyber resilience.[110] The cybersecurity Order additionally places emphasis on the need for cybersecurity risk management and specialists to create a consistent security protocol and increase the federal government's accountability for cybersecurity issues.[111]

President Obama stated in the 2015 State of the Union that he hopes that cybersecurity will come to the forefront of Congress' agenda, especially due to the recent cybersecurity issues faced by American companies, such as Sony Entertainment Pictures, Home Depot and Target, have faced.[112] As detrimental issues, such as insider trading transactions, can arise with weak cybersecurity, the federal government should impose requirements to protect the US government and private companies from facing cybersecurity breaches.

Why The Current Model No Longer Covers All Types of Insider Trading

The current insider trading laws and case precedents do not directly deal with online security breaches and the release of private and confidential information, despite living in an era where all companies and people store a vast of information online. These online databases are generally accepted to be private and secure, and therefore only available to those who have access and a fiduciary duty to the company.[113] Recent events are proving that these secure databases are vulnerable to security breaches; therefore modified laws are warranted to ensure that those who do wrong in this novel manner are charged.[114]

Currently, companies have no obligation to report cyber intrusions to law enforcement.[115] Furthermore, most companies do not want to publicize that they have been compromised and attempt to deal with the problem internally.[116] In March of 2014, SEC Chairwoman Mary Jo White stated that public companies have an obligation to report "material risks to their business – including risks related to data security like hacking and identity theft."[117] Chairwoman White goes on to state that reporting this gives investors full

---

[109] Zeichner, *supra* note 104.

[110] EO 13636: *Improving Critical Infrastructure Cybersecurity*, GSA.GOV (last updated, Sept. 30, 2014), http://www.gsa.gov/portal/content/176547.

[111] *Id.*

[112] Shear, *supra* note 107.

[113] Lauren C. Williams, *The Heartbleed Bug Reveals We're Willing To Give Up Online Security To Feel More Connected*, THINK PROGRESS (Apr. 12, 2014), http://thinkprogress.org/culture/2014/04/11/3425310/what-the-heartbleed-bug-says-about-our-interconnectivity.

[114] Green, *supra* note 21; Sherwin, *supra* note 1; Bill Buchanan, *Heartbleed bug: insider trading may have taken place as shares slid ahead of breaking story*, THE CONVERSATION (Apr. 30, 2014), http://theconversation.com/heartbleed-bug-insider-trading-may-have-taken-place-as-shares-slid-ahead-of-breaking-story-26026.

[115] Zoe Argento, *Killing The Golden Goose: The Dangers of Strengthening Domestic Trader Secret Rights in Response to Cyber Misappropriation,* 16 YALE J. L. & TECH. 172, 216 (2013-14).

[116] *Id.*

[117] Jordan Thomas & Vanessa De Simone, *Cybersecurity - Growing Technological Threats Raise New Issues for Investors and the SEC*, SEC WHISTLE BLOWER ADVOCATE (May 1, 2014), http://www.secwhistlebloweradvocate.com/secwhistleblowradvocate/cybersecurity-growing-technological-threats-raise-new-issues-for-investors-and-the-sec; Mary Jo White, *Opening Statement at SEC Roundtable on*

disclosure on the company, as well as motivates companies to continuously update their cybersecurity.[118] Despite the SEC's recent comments, the private sector still fails to disclose security breaches in fear of losing investors and clients.[119]

Due to the case precedent holding that tippees are only liable for insider trading if a fiduciary duty is derived from the tipper's duty, we need to both close the gap of cybersecurity, and insider trading loopholes. Should society fail to amend and strengthen the laws, wrongdoers are going to trade on material nonpublic information with the intent to deceive.

III. CURRENT LAWS AND HOW THEY ARE BEING CIRCUMVENTED

Lack of Legislation Requiring Cybersecurity Standards

Currently, there are minimal cybersecurity requirements in the United States and therefore no attention is given in this Note regarding how wrongdoers are circumventing cyber laws.[120] An example of how vulnerable the United States has made itself by the lack of cybersecurity requirements is demonstrated through the November 2014 Sony Pictures Entertainment ("Sony Pictures") hack.[121] Sony Pictures employees saw a message on their computers stating that the company has been hacked by a group known as the Guardian of Peace ("GOP") and that a copious amount of data had been compromised.[122]

In December 2014 after a thorough investigation, the Federal Bureau of Investigations determined that the North Korean government executed this cyberattack.[123] Despite this being an international cybercrime, there is no reason that hackers within the United States could not have accomplished a hack of such magnitude. Furthermore, there is no certainty that any cybersecurity requirements applicable to companies, such as Sony Pictures, could have protected the company against such an invasive cybercrime. This public and very recent cyberattack demonstrates just how susceptible our society is to such threats.

The Sony Pictures stock price was not greatly affected by the hack, as the hackers released some of the documents to the public and kept the rest private.[124] The stock price was further kept stable due to the actions of the recently hired Chief Financial Officer.[125] Additionally, society believes that the company can bounce back from the hack since such

---

Cybersecurity, SEC (Mar. 26, 2014), http://www.sec.gov/News/PublicStmt/Detail/PublicStmt/1370541286468#.VE6D675W0sq.

[118] Thomas & De Simone, *supra* note 117; Mary Jo White, *supra* note 117.

[119] Joseph Menn, *Exclusive: Hacked companies still not telling investors*, REUTERS (Feb. 2, 2012), http://www.reuters.com/article/2012/02/02/us-hacking-disclosures-idUSTRE8110YW20120202.

[120] *See generally* FISCHER, *supra* note 15.

[121] Dave Lewis, *Sony Pictures Hacked And Blackmailed*, FORBES (Nov. 24, 2014), http://www.forbes.com/sites/davelewis/2014/11/24/sony-pictures-hacked-and-blackmailed.

[122] *Id.*

[123] *Update on Sony Investigation*, FBI.GOV (Dec. 19, 2014), http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

[124] James Cook, *Sony Hackers Have Over 100 Terabytes Of Documents. Only Released 200 Gigabytes So Far*, BUSINESSINSIDER (Dec. 16, 2014) http://www.businessinsider.com/the-sony-hackers-still-have-a-massive-amount-of-data-that-hasnt-been-leaked-yet-2014-12.

[125] Ansuya Harjani, *Forget hacking drama, Sony stock to rise 40%: analyst*, CNBC (Dec. 23, 2014), http://www.cnbc.com/id/102290728.

bumps are factored in the movie industry to account for unsuccessful movies and other potential hindrances.[126] Regardless of the stock aspect of the hack, Sony Pictures faced what is turning out to "possibly [be] the costliest [hack] ever for an American company."[127] It is estimated that this breach could cost Sony Pictures over $100 million.[128]

The hackers have released a vast amount of private information, from unreleased movies to information regarding employees (salary, social security numbers, addresses, etc.) to private email exchanges of the executives.[129] The GOP hackers have stated that they only released about 235 gigabytes of the 100 terabytes of material they have taken from the Sony Pictures databases.[130] Further, this breach has resulted in current and former employees suing Sony Pictures for security breach, stating that the company failed to adequately ensure that all private employee information was protected.[131] The suit alleges that Sony Pictures was negligent in failing to prepare for a cyberthreat despite the numerous past hacks.[132]

Past and present employees of Sony Pictures have faced an injustice and are dealing with it through the class action suits, but what if this were an insider trading issue? The market currently does not have a remedy if hackers, such as the Sony Pictures hackers, passed the stolen information onto others who traded based on the information. Are these the type of individuals that we are attempting to protect with the rigidity of the current insider trading requirements?

The *Dorozkho* case holding can only support for a hacker tipper's reliance on stolen material nonpublic information to trade. *Dorozkho* did not entertain what would happen if the tipper were to pass the information on to a tippee who relied on it, as the *Dorozkho* court was able to convict without a fiduciary duty. What about if the GOP hackers passed material nonpublic information onto a select few people who did then rely on the information and trade? There is no value in protecting these wrongdoers and allowing them to profit off companies and devalue the intentions of security investments.

Society has now been looking at the government and its agencies to deal with the disaster that resulted from the November 2014 Sony Pictures hack. The SEC is attempting to notify those within its reach about the threat of cybersecurity and its impact on stocks.[133] Chairwoman Mary Jo White states that protecting online investments from cyberthreats is a main focus of the SEC. Chairwoman White also holds that by government agencies working together, the threat of cyberattacks can be minimized.[134]

---

[126] Jack Hough, *Sony Stock Is a Bargain Despite Hack Attack*, BARRONS (Dec. 17, 2014), http://online.barrons.com/articles/sony-stock-is-a-bargain-despite-hack-attack-1418916503.

[127] Harjani, *supra* note 125.

[128] Lisa Richwine, *Cyber attack could cost Sony studio as much as $100 million*, REUTERS.COM (Dec. 9, 2014), http://www.reuters.com/article/2014/12/09/us-sony-cybersecurity-costs-idUSKBN0JN2L020141209.

[129] Cook, *supra* note 124; Steve Musil, *Unreleased Sony movies leaked to file-sharing sites after hack*, CNET (Nov. 30, 2014), http://www.cnet.com/news/hackers-leak-new-sony-movies-to-file-sharing-sites.

[130] Cook, *supra* note 124.

[131] Seth Rosenblatt, *Sony sued by former employees over hack*, CNET.COM (Dec. 16, 2014), http://www.cnet.com/news/sony-sued-by-current-former-employees-over-hack.

[132] Ralph Ellis, *Lawsuits say Sony Pictures should have expected security breach*, CNN.COM (Dec. 20, 2014), http://www.cnn.com/2014/12/20/us/sony-pictures-lawsuits.

[133] Press Release Washington, DC, *SEC Alerts Investors Industry on Cybersecurity*, SEC. GOV (Feb. 3, 2015), http://www.sec.gov/news/pressrelease/2015-20.html#.VNaw5kJW2SE.

[134] *Id.*

As discussed, there is an enormous and unacceptable gap in modern society's necessary legislation regarding cybersecurity. On the other hand, there are insider trading laws which we can turn to and assess how they are being eluded through cyberhacking.

How Insider Trading's Laws Are Currently Being Evaded

In the *Dirks v. SEC* case, the Supreme Court stated that proof that material nonpublic information was disclosed in breach of the tipper's duty of confidentiality and for personal benefit is required to show a breach of fiduciary duty.[135] The personal benefit requirement that is necessary to establish a breach of fiduciary duty has been applied quite liberally. Furthering a friendship[136] and other profit types beyond monetary[137] are examples of what has been considered a personal benefit. Furthermore, the *Dirks* Court broadmindedly stated that the tippee is liable when it can be established that the tippee merely *should know* that the tipper has breached their fiduciary duty.[138]

The lenient language of the seminal *Dirks* case has allowed the SEC to hold many people accountable for their unlawful actions. The Second Circuit in December 2014 has greatly added to the burden of showing insider trading with the holding of *United States v. Newman*.[139] The Second Circuit held that a tippee is only liable for insider trading when they had knowledge that the tipper gained a personal benefit and when the tipper breached their fiduciary duty and thus passed that breach onto the tippee.[140]

In the *Newman* case, the two defendants tippees were portfolio managers at hedge fund companies.[141] The government argued that the corporate insiders passed that material nonpublic information to analysts at hedge fund companies, and these analysts passed it onto the defendants, directly and indirectly. The government provided evidence that the defendants traded on the said material nonpublic information and collectively earned nearly $70 million in profits.[142]

Due to the rigidity that resulted from the Second Circuit's interpretation of the Dirks test, the *Newman* Court found that there was insufficient evidence in the matter to prove that the tippees (defendants) had actual knowledge that the tipper gained a personal benefit. Due to the government's failure to meet its burden to show that illegal insider trading occurred, the matter was dismissed with prejudice.[143]

Even after considering the 2014 *Newman* case[144] and the 2009 *Dorozkho* case[145], the SEC still treads in murky water when it comes to charging cyberhackers with insider trading, let alone the ability to charge the tippees that can result from the hackers actions. Dorozkho was found to be within the jurisdiction of insider trading as the SEC successfully argued that

---

[135] Dirks v. SEC, 463 U.S. 646, 647 (1983).

[136] *See* SEC v. Obus, 693 F.3d 276, 291 (2d Cir. 2012).

[137] William McLucas et al., *Recent Insider Trading Decision*, MONDAQ (Dec. 29, 2014).

[138] *Dirks*, 463 U.S. at 660 (1983) (emphasis added).

[139] United States v. Newman, 773 F.3d 438 (2d Cir. 2014).

[140] *Id.* at 450.

[141] *Id.*

[142] *Id.* at 443.

[143] *Id.* at 455.

[144] *Id.*

[145] SEC v. Dorozhko, 574 F.3d 42 (2d Cir. 2009).

Dorozkho's misrepresentation during the hacking process was deceptive fraud, enough to be within the insider trading rules despite the lack of a fiduciary duty.[146] The Second Circuit agreed with the SEC but remanded the issue of whether misrepresentation is deceptive theft.[147] Despite the SEC successfully arguing that misrepresentation is deceptive fraud matter based on the specific facts of this case, the precedent established is not convincing enough or fully encompassing of all future cyberhacking cases. Furthermore, the *Dorozkho* holding applies to those who hack and then trade based on the information, but what happens when the hacker pass on the information? How can a tippee be held liable without the fiduciary duty being passed along with the material nonpublic information?

From the holding of the recent judgment of the *Newman* case, tippees resulting from information gained via a cyberhacker will likely not be aware of a personal benefit gained by the hacker tipper. The 'tippee knowledge of tipper personal benefit' requirement seems quite rigid and unnecessary as it protects many who should not be afforded that comfort. Both the traditional tipper and hacker (non-traditional) tipper can pass information onto another (a tippee) without gaining a personal benefit, let alone the tippee's knowledge of the personal benefit. Are we content with a tippee trading based on the material nonpublic information if the tippee does not gain actual knowledge of the tipper's benefit?

Based on this rationale from *Dorozkho*[148] and *Newman*[149], even if the SEC is able to get the hacker for fraudulent acts, the tippees who are affecting the validity of the market would have the freedom to trade. These types of actions are clearly against the public policy and intention of insider trading laws, but when looked at closer, fail to meet all the requirements for insider trading.

The Hacker's Loophole Becomes Apparent with Recent Events

Coupling the recent Sony Pictures hack and the online security breach bugs into context; along with the insider trading laws movement in the Second Circuit, through the *Dorozkho*[150] and *Newman*[151] cases, there is a vast problem that needs to be addressed immediately. Cyber laws need to be intertwined with securities laws to further strengthen insider trading regulations. Without adequate cyber laws the securities laws may be left with a weakness.

Why are we holding *personal benefit* to be a determinative factor for insider trading actions? Why are we leaving a realm of unknown application regarding insider trading transactions via hackers and the resulting tippees? Should online hackers who steal material nonpublic information about companies and those who the information is passed on (potential tippees), be allowed to trade and gain based on the information? Are these not the exact type of intentional misconduct that security laws are supposed to prevent?

There is an apparent means of evasion between the intentions of insider trading laws and how they are being applied, especially in light of information obtained through

---

[146] *Id.* at 49-51.

[147] *Id.* at 51.

[148] *Dorozhko*, 574 F.3d.

[149] *Newman*, 773 F.3d.

[150] *Dorozhko*, 574 F.3d

[151] *Newman*, 773 F.3d.

cyberspace. Laws are ever-changing and are to solve difficulties that come to light, thus we must apply them as society develops for the better but opens to greater flaws. Now that society can clearly identify that there is a problem with cybersecurity and its connection to insider trading, it is time for the weakness to be eliminated and the wrongdoers accountable for their objectionable actions.

IV. HOW NECESSARY CHANGES IN THE LAW WILL COMBAT THIS NEW TYPE OF INSIDER TRADING

Time for a Change

First, changes are evidently needed to close the large gap between the interpretation of insider trading rules and the new realm of cyberhacking. Cybersecurity is a problem that society has been forced to look at in the past year, after years of avoidance.[152] Society saw some of the largest and most destructive cyberhacks in 2014. From the recent events it has become clear that changes should have been made to account for cyberhacking possibilities prior to the vulnerability being violated. Despite the fact that we cannot change the past, we can ensure that our future is guarded from such avoidable acts. We now have the opportunity to make amendments to our current laws to account for the exposed and future prospective weaknesses.

The stock market holds great value in the economy and has the ability to change the course of business within a few days as evidenced by the recent 2008 Stock Market Crash, and also the infamous 1929 Wall Street Stock Market Crash. Due to the recent cyberhacks, it has evidently been revealed that there is vulnerability, and therefore it should be resolved before the vulnerability is compromised and society faces an event comparable to that of the 2008 stock market crash, or even one as great as the 1929 crash. As the SEC was created with the intention of protecting society from instable markets, the SEC has a burden of remediating this issue, as does Congress. The integrity of the stock market can be easily undermined, as long as this existing weakness remains.

Both the international element and lack of cybersecurity standards add complications for the ability to eliminate cyberhacking. Therefore, until we can curb cyberhacking as a whole, we must ensure that we prosecute any insider trading that may result. There are various ways in which we can address and remediate the issues regarding hacker tippers and tippees who may rely on information obtained through the hacking.

Adding a Cyberhacking Caveat to Rule 10b-5

One approach would be to amend the SEC rules to forbid insider trading with reliance on material nonpublic information taken via hacking, and the tippees who may result. The SEC has the jurisdiction to charge on matters dealing with the purchase of a security through manipulative or deceptive device.[153] Hacking is an intentional act and requires

---

[152] *State of the Union – 2015 Full Transcript*, CNN (Jan. 20, 2015), http://www.cnn.com/2015/01/20/politics/state-of-the-union-2015-transcript-full-text.

[153] 15 U.S.C. § 78j(b) (2012).

manipulation,[154] therefore the SEC has jurisdiction to charge for insider trading that results from hackers gaining information.[155]

Tippers and tippees who result from insider trading via hacking can be accounted for by adding a subsection under Rule 10b-5. Though it could be argued that *Dorozkho* has provided a degree of precedence for hackers, it is not clearly effective, nor does it account for tippees who may follow. Additionally, the holding from *Dorozkho* is further weakened by the *Newman* holding, requiring the tippee to have knowledge of the personal benefit that the tipper is gaining from passing the material nonpublic information. Therefore despite the breakthrough that the SEC had with the *Dorozkho* holding, it shows no promise that all hackers will fall within the same fact pattern, let alone the hacker's tippees. As the *Dorozkho* case, especially with the *Newman* holding, failed in successfully setting a strong precedent for encompassing hackers within the SEC insider trading regulations, there is clear evidence showing a need for a specific rule to make such activity illegal.

Tippees should be liable for insider trading via hacking even without knowing the tipper's personal benefit[156] or even a finding of fiduciary duty.[157] The current determinative factors for finding insider trading do not encompass the intent of the laws. The intent of insider trading laws should be revisited to determine the best method on how to amend the law to encompass the fluidity of society. As the SEC has stated, the intent of insider trading laws are to ensure the veracity of the markets, separating the tipper and tippee in such situations will ensure that tippees do not evade insider trading rules by this current method to circumvent the laws.

Tippee Liability Absent Identified Tipper

As argued above in favor of the Rule 10b-5 caveat for hackers, there are also some potential issues. Due to the international and extreme anonymity of cyberhackers, there may be a very minimal likelihood of being able to identify the hackers,[158] let alone assert sufficient personal jurisdiction over them to bring them into US courts.[159] Noting the personal jurisdiction issue, it should also be revealed that personal jurisdiction has been asserted over an international defendant through the federal long-arm statute of Federal Rule of Civil

---

[154] *See* n. 22.

[155] *But 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) (Mr. Denny argues that hacking should only be applied in instances where the hacker "guess[es] a password [], exploit[s] a computer code, or otherwise deceive a computer [] contrary to its intended usage. *Id.*

[156] US v. Newman, 773 F.3d 438, 454 (2d Cir. 2014).

[157] Dirks v. SEC, 463 U.S. 646, 678-79 (1983).

[158] Andres A. Muñoz, *United States v. Jarrett (Decided July 29, 2003)*, 1 N.Y.L. SCH. L. REV. 411, 419 (2005).

[159] Havlish v. Royal Dutch Shell PLC, 2014 WL 4828654, at *2 (S.D.N.Y. Sept. 24, 2014). This case holds that the petitioners hold the burden of proving that there is sufficient personal jurisdiction of the court over the defendant. Fed. R. Civ. Pro. 12(b)(2) (2012). To ease the petitioner, the court finds that the petitioner's assertions are deemed to be true unless invalidated by the defendant. *Havlish,* WL 4828654, at *2.

Procedure 4(k)(2), [160] when the necessary minimal contacts to the state has been established.[161]

In the matter of MacDermid, Inc. v. Deiter,[162] the Second Circuit found that the Court had personal jurisdiction over a Canadian defendant who hacked into the computers located in Connecticut, of a company also based in Connecticut.[163] The Court stated that the minimal contacts were satisfied as the defendant hacked into servers, which were located in Connecticut; therefore that defendant's act brought her within the federal long-arm statute and that of the state, as the statute only requires that the device [computer] be within the state.[164] Further, in this matter, the minimal contacts were sufficient as the defendant was aware of the fact that the servers that she was hacking into were located in Connecticut.[165]

Despite the holding established by *MacDermid, Inc.*, establishing personal jurisdiction over a hacker can only be found once the hacker has been identified.[166] Again, due to the high anonymity of hacking, that may be exceedingly unlikely.[167] As the current SEC rules state that a tipper must be identified prior to the ability of charging a tippee, holding the hackers as tippers may not always allow for liability to be asserted on tippees who may result. Given the uncertainty of constantly identifying hackers and thus tippers in insider trading actions that result from cyberhacking, removing the barrier of identifying the tipper when attempting to assert an insider trading charge against obvious tippees would further ensure that insider trading rules are upheld to their broadest application.

Cyberhacking Prevention Burden on Companies

A third option which can help confirm that tippees will be held accountable, regardless of whether this is an identifiable tipper or not, is to place more of a burden on the companies. This option accounts for both the insider trading vulnerability and the lack of cybersecurity regulations. Currently, with the lack of cybersecurity requirements and the rigid definition for insiders, companies are not held to a high standard of responsibility. Holding the companies as the tippers can strengthen the current low standard. Insider trading resulting from cyberhacking can bypass its current loophole by injecting the company in place of the tipper. If the burden of allowing hacking and thus the transmission of material nonpublic information are placed on the company, the tippees can be held liable for their actions.

Under such a regulation, the hackers would be the tippees of the company as the company clearly has a fiduciary duty to itself to keep material nonpublic information confidential. The hacker tippees are then passed information from the company tipper through deliberate means or reckless disregard to protect its confidential information. The company can be said to gain a material benefit of falsely inflated stock prices, which can be an unintended result of insider trading. Further, those who the hacker tippee passes the

---

[160] Fed. R. Civ. Pro. 4(k)(2). (2012).

[161] *See* World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286 (1980); Int'l Shoe Co. v. Wash., 326 U.S. 310 (1945).

[162] 702 F.3d 725, 727 (2d Cir. 2012).

[163] *Id.*

[164] *Id.* at 728-29.

[165] *Id.* at 730.

[166] Dirks v. SEC, 463 U.S. 646, 647 (1983).

[167] Muñoz, *supra* note 158.

information onto would become remote tippees and carry the fiduciary duty that the hacker obtained from the company as the original tipper.

Security breaches, the Internet as a host, and insider trading are issues that have been around for a while, though they have been ill prepared for. If such security breaches and insider trading were more apparent, public companies would have been spending more and doing whatever else necessary to ensure that their private and confidential information remain that way until they desire to release it. In comparison, if companies could have foreseen these breaches, they could have taken the information offline and stored it in a different manner.

Given that companies are evidently not adhering to the caliber needed to keep hackers barred, the law should both hold them accountable for their ineffectiveness while raising the norm by implementing cybersecurity standards. Holding companies as tippers in such instances, where tippees are relying on material nonpublic information obtained through cyberhacking will force companies to ensure that their information is secure. The implementation of this change would require security experts and companies to ensure that they have the best security, maintenance and ability to update for potential threats ahead of hackers. On the other hand, it will also protect companies by having the means to reach tippees, though also facing the issue of the tipper (itself) breaching its fiduciary duty. Though again, the intent of insider trading laws is to maintain the integrity of the market and therefore it is necessary that the tippees be reached and charged rightfully.

Society's call for cybersecurity standards is necessary and though the risks of cyberhacking were visible prior to the many recent incidents, 2014 saw a glimpse of the true extent of such acts. The struggles from the past years must drive this issue to the forefront of Congress' and the SEC's attention. There are a great deal of benefits of the exponential technology growth in recent times, though we cannot forget to be mindful of the potential issues that come along with that progression.

Federal Laws

The call for mandated changes to the insider trading laws and its relation to cybersecurity laws must be uniform across the country to ensure its greatest strength of enforcement. State borders are becoming less apparent in all respects, though noticeably and understandably in cyberspace. If each state or court jurisdiction were to have its own laws and applications for cyberhacking insider trading issues, or even cybersecurity as a whole, we will undoubtedly be faced with numerous issues by repairing this one issue. Insider trading laws and other security regulations are already applied differently by each circuit court, a problem that we need not add to.[168]

If the insider trading laws in respect to cyberhacking are not consistent across the nation, then we will likely see illegal insider trading via hacking within the jurisdictions that fail to apply the laws with vigor, or tolerate loopholes for tippees to evade insider trading rules with. Furthermore, we will possibly see a higher number of actions within the strict jurisdictions by the SEC bringing suits within those jurisdictions when possible. Looking back at the original intent, having varying definitions and applications would weaken the reputation of the stock markets, a result that we are attempting to avoid.

---

[168] Maura K. Monaghan, *An Uncommon State of Confusion: The Common Enterprise Element of Investment Contract Analysis*, 63 Fordham L. Rev. 2135, 2158 (1995).

In regard to cybersecurity, this is a national issue at the very least, not merely a jurisdictional issue. The lack of cybersecurity regulations, especially in regards to security regulations and specifically insider trading, is a positive, in the sense that it allows us to start from a clean slate. We have now been in the cyber world for a long duration, which allows expert to explore and understand the intricate cyber issues that can arise. Congress should take this opportunity to pass legislation to encompass the diverse aspects in which cyberspace exists in our lives. There are relatively no borders in cyberspace, and therefore there should be none within a nation for the laws that apply to cyberspace.

CONCLUSION

Sony Pictures hack and the Internet security bugs have proven that hackers are infiltrating every aspect of our society, from entertainment to financial platforms. Society has become more and more dependent on the Internet and the information we choose to transmit online. As cyber space continues to become more ingrained in our everyday lives, we must protect this new space; otherwise we will continue to see the wrath of what hackers are capable of.

The SEC is currently posed with a new type of insider trading. If hackers are able to infiltrate the servers of public companies to gain material nonpublic information, they are also able to pass that information onto tippees. Hackers do not have a confidential relationship with the company whom they are taking information from without permission; therefore hackers have no fiduciary duty to the company.[169] Tippees who obtain material nonpublic information from hacker tippers are then able to rely and trade on the material nonpublic information without a fiduciary duty to the company being placed on them.

Insider trading transactions resulting from security breaches and hackers pose a very genuine concern that may affect the markets unknowingly. Security breaches can be difficult to notice and can easily be anonymous.[170] The anonymity of potential hacker tippers creates an issue for the SEC's ability to charge tippees, as the tippee has no insider trading liability without the proof of the tipper's breach of fiduciary duty.

Given the strength that the stock markets have proven to possess in the United States, we must ensure the integrity of the market by closing all gaps. Insider trading laws must be amended to account for hackers and their potential tippees by creating a caveat for hackers being tippers within the SEC regulations regarding insider trading. The laws can additionally be altered to remove the requirement of identifying tippers prior to charging tippees with insider trading. Furthermore, insider trading regulations can also be amended to encompass hackers by holding the companies as tippers, the hackers as tippees, and those whom obtain information from the hacker and rely on the information as remote tippees. This third option will also ensure that public companies have strong cybersecurity measures, as the current lack of cybersecurity regulations is an added component in the issue of insider trading via hackers.

---

[169] SEC v. Dorozhko, 574 F.3d 42, 48 (2d Cir. 2009).

[170] Muñoz, *supra* note 158.