I. SEC Enforcement Efforts with Insider Trading and Cybersecurity

A. Introduction

Illegal insider trading occurs when a security is purchased or sold "in breach of a . . . relationship of trust and confidence, while in possession of material, nonpublic information about the security."[1] Cybersecurity is defined as "the body of technologies, processes and practices designed to protect networks, systems, computers, programs and data from attack, damage or unauthorized access."[2] In recent years, cyber threats have increasingly posed "non-discriminating risks across our economy to all of our critical infrastructures, our financial markets, banks, intellectual property, and . . . the private data of the American consumer."[3] The U.S. Defense Intelligence Agency has identified cyber threats as posing an even greater global risk than terrorism.[4] Though the risk of a cyber attack jeopardizes the private data of every industry, the financial services sector in particular remains vulnerable to cyber criminals who wish to obtain confidential data in order to utilize it to their financial gain, through techniques like insider trading.[5] The

---

[1] 17 CFR § 240.10b5-1(a) (2014); *Insider Trading*, SEC. & EXCH. COMM'N, http://www.sec.gov/answers/insider.htm [http://perma.cc/4CNV-SB65].

[2] SEC. & EXCH. COMM'N, CF DISCLOSURE GUIDANCE: TOPIC NO. 2 CYBERSECURITY (2011), *available at* https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm [http://perma.cc/J2ME-5VHQ] [hereinafter CF DISCLOSURE GUIDANCE] (citing *Cybersecurity Definition*, WHATIS.COM, http://whatis.techtarget.com/definition/cybersecurity.html (last visited Sept. 25, 2015)).

[3] *Cybersecurity Roundtable*, SEC. & EXCH. COMM'N, Mar. 26, 2014, at 7-8 (transcript available at http://www.sec.gov/spotlight/cybersecurity-roundtable/cybersecurity-roundtable-transcript.txt [http://perma.cc/A6JL-Y46R]).

[4] *Id.* at 8 ("Cyber threats are of extraordinary and long-term seriousness. They are first on the Division of Intelligence's list of global threats, even surpassing terrorism.").

[5] *See e.g.*, *Combating the Biggest Cyber Threats to the Financial Services Industry*, LOCKHEED MARTIN CORP. 3 (2015), http://cyber.lockheedmartin.com/hubfs/docs/Technical_Papers/WP-Financial_Services_Combatting_Cyber_Threats.pdf?t=1448048345856 [http://perma.cc/84YS-JJUV] (finding that "market manipulation and

Securities and Exchange Commission (SEC), which polices insider trading,[6] has attempted to curtail cyber attacks in the financial marketplace through a variety of policy and enforcement measures.[7]

This article will examine the current and projected enforcement efforts of the SEC over the intersection of insider trading and cybersecurity. Part I illustrates the extent the SEC has demonstrated jurisdiction over cybersecurity and insider trading, and its recent policy initiatives. Part II examines the history of the SEC's cybersecurity enforcement efforts. Part III describes developing cases against large-scale insider trading operations that raised interest in the regulation of cybersecurity. Part IV outlines measures that companies can take to mitigate the risk of cyber threats. Finally, Part V provides an argument for increased regulation of the cybersecurity of third-party service providers.

B. SEC Jurisdiction and Policy Guidance Relating to Cybersecurity

Though insider trading has long been squarely within the SEC's enforcement priorities,[8] the SEC has only explicitly demonstrated that "cybersecurity is within its jurisdiction" in the past four years.[9] In October 2011, the SEC's Division of Corporation Finance released guidance pertaining to corporate disclosure obligations in connection to risks and incidents relating to cybersecurity.[10] This guidance places on public companies an affirmative obligation to disclose "material information regarding cybersecurity risks and cyber incidents" when necessary to make

---

unauthorized stock trading" deriving from cyber attacks are "common risks" facing financial firms).

[6] *See Insider Trading*, *supra* note 1.

[7] *See e.g.* CF DISCLOSURE GUIDANCE: TOPIC NO. 2 – CYBERSECURITY, *supra* note 2. *See* generally Cybersecurity Roundtable, *supra* note 3.

[8] *See Insider Trading*, *supra* note 1.

[9] *See* Alexis Ronickher, *Cybersecurity Front and Center in SEC's Recent $100M Insider-Trading Enforcement Action,* KATZ, MARSHALL & BANKS SEC WHISTLEBLOWER BLOG (Aug. 28, 2015), http://www.secwhistleblowerblog.com/cybersecurity-front-and-center-in-secs-recent-100m-insider-trading-enforcement-action/ [http://perma.cc/5VTC-DU85].

[10] CF DISCLOSURE GUIDANCE, *supra* note 2.

"other required disclosures . . . not misleading."[11] According to Mary Jo White, Chairwoman of the SEC, "the SEC's formal jurisdiction over cybersecurity is directly focused on the integrity of our market systems, customer data protection, and disclosure of material information."[12]

In March 2014, the SEC hosted a cybersecurity roundtable that primarily focused on the risks cyber attacks pose to public companies and to the capital markets.[13] The SEC also issued guidance in April 2015 underscoring the SEC's attitude that implementing robust cybersecurity measures in the financial industry is "an important issue," and recommends various protective measures.[14] Moreover, the SEC noted in its guidance that "[c]yber attacks on a wide range of financial services" companies demonstrated the need for these companies to review their cybersecurity plans.[15]

C. Cybersecurity Enforcement Efforts

Prior to 2015, the SEC had not enforced an action against a party for failures related to inadequate cybersecurity.[16] In September 2015, the SEC accepted a settlement offer from R.T. Jones Capital Equities Management, Inc. to conclude proceedings against R.T. Jones for its "failure to adopt written policies and procedures reasonably designed to protect customer records and information, in violation of Rule 30(a) of Regulation S-P."[17] Rule 30(a) of Regulation S-P requires "[e]very broker, dealer, and investment company, and every investment adviser registered with the [SEC to implement] written policies and procedures" to "[i]nsure [sic] the

---

[11] *Id.*
[12] *Cybersecurity Roundtable*, *supra* note 3, at 8.
[13] *See generally id.* at 170; *infra* notes 55-56 and accompanying text.
[14] *See* SEC. AND EXCH. COMM'N, CYBERSECURITY GUIDANCE (2015), *available at* http://www.sec.gov/investment/im-guidance-2015-02.pdf [http://perma.cc/5L9B-D4PU] [hereinafter CYBERSECURITY GUIDANCE] (acknowledging the increasing use of technology by funds and advisors and providing methods to protect the confidential and sensitive information of investors and advisory clients); *infra* notes 57-58 and accompanying text.
[15] CYBERSECURITY GUIDANCE, *supra* note 14.
[16] *See* Ronickher, *supra* note 9.
[17] R.T. Jones Capital Equities Mgmt., Inc., Investment Advisers Act of 1940 Release No. 4204, 2015 WL 5560846, at *1 (Sept. 22, 2015) [hereinafter R.T. Jones].

security and confidentiality of customer records and information."[18] R.T. Jones allegedly stored sensitive client information on an external web server without having such policies and procedures in place.[19] In July 2013, the firm's web server was hacked by an unknown intruder, thus exposing the personal information of more than 100,000 individuals to the risk of potential theft.[20] The SEC determined that it was in the public interest to impose monetary sanctions against R.T. Jones.[21] These sanctions included a $75,000 civil penalty and an order to cease and desist from further violations.[22]

The SEC's enforcement action against R.T. Jones reflects the agency's recent mission to make issues related to cybersecurity a "key enforcement priority."[23] The SEC took enforcement action in this case despite the lack of "actual economic harm" and despite the "prompt remedial actions" taken by R.T. Jones to "inform and protect its clients, investigate the breach, and ensure future breaches did not recur."[24] The R.T. Jones case is "almost certainly only the first of many such cases."[25]

Additionally, the SEC has previously enforced an action against a hacker who illegally obtained insider information and used that information for his personal gain.[26] In 2007, the [SEC] filed a complaint charging Oleksandr Dorozhko with hacking into the computer network of an investor relations firm to access earnings information for IMS Health.[27] The complaint further alleged that he learned of "nonpublic information regarding . . . negative earnings by IMS Health," and purchased 630 put options on IMS stock, realizing

---

[18] *See* 17 C.F.R. § 248.30 (2005).
[19] *See* R.T. Jones, *supra* note 17.
[20] *Id*. at *2.
[21] *Id*. at *4.
[22] *Id*. at *4.
[23] *See* Dallas Hammer, *SEC Enforcement Action Portends Rewards for Cybersecurity Whistleblowers*, ZUCKERMAN LAW (Sept. 26, 2015), https://www.zuckermanlaw.com/sec-enforcement-action-portends-rewards-for-cybersecurity-whistleblowers/ [https://perma.cc/Q8H4-CMAU].
[24] *Id*.
[25] *Id*.
[26] *See* Press Release, Sec. & Exch. Comm'n, SEC Obtains Summary Judgment Against Computer Hacker For Insider Trading (Mar. 29, 2011), *available at* https://www.sec.gov/litigation/litreleases/2010/lr21465.htm [http://perma.cc/UX8U-N7UJ].
[27] *Id*.

"profits of approximately $287,346" upon their subsequent sale.[28] Specifically, the complaint alleged "that Dorozhko violated Section 10(b) of the Securities Exchange Act of 1934 and Rule10b-5 thereunder by using 'fraudulent devices, schemes, or artifices, which may include, but are not limited to, hacking into computer networks or otherwise improperly obtaining electronic access to systems that contained [nonpublic] information.'" [29] The SEC successfully obtained summary judgment against Dorozhko in March 2010.[30]

D. Recent Developments

1. *SEC v. Dubovoy*

The SEC recently charged thirty-four defendants for their involvement in an "unprecedented hacking and trading scheme"[31] in which stolen information regarding corporate earnings was illegally used for the defendants' monetary gain.[32] The SEC alleges that "two of the defendants . . . hacked into newswire services and transmitted the stolen data to a web of international traders."[33] By having access to the information before it was released publicly, the traders allegedly made more than $100 million in illegal profits between 2010 and 2015.[34]

The SEC claimed that Ivan Turchynov and Oleksandr Ieremenko led the operation by using advanced hacking techniques to steal hundreds of corporate earnings announcements from two or

---

[28] *Id*.
[29] *Id*.
[30] *Id*.
[31] Press Release, Fed. Bureau of Investigation, Nine People Charged in Largest Known Computer Hacking and Securities Fraud Scheme (Aug. 11, 2015), *available at* https://www.fbi.gov/newyork/press-releases/2015/nine-people-charged-in-largest-known-computer-hacking-and-securities-fraud-scheme [https://perma.cc/WS2H-UFH4].
[32] Press Release, Sec. & Exch. Comm'n, SEC Charges 32 Defendants in Scheme to Trade on Hacked News Releases (Aug. 11, 2015), *available at* https://www.sec.gov/litigation/litreleases/2015/lr23319.htm [http://perma.cc/84L4-PP6Q].
[33] Press Release, Sec. & Exch. Comm'n, SEC Obtains $30 Million From Traders Who Profited on Hacked News Releases (Sept. 14, 2015), *available at* http://www.sec.gov/news/pressrelease/2015-191.html [http://perma.cc/W36A-6JJE].
[34] *Id*.

more newswires.[35] The SEC further alleged that the pair spread the stolen information to traders around the world.[36] The traders then used this information in a short time frame to place illegal trades in securities.[37]

In a parallel action, prosecutors in Brooklyn, New York and Newark, New Jersey announced criminal charges against nine of the defendants.[38] This action represented "the first time [that] criminal charges have been brought for a securities fraud scheme involving hacked inside information."[39]

The SEC announced on September 14, 2015 that two of the participants in the operation agreed to turn over $30 million in ill-gotten gains.[40] Andrew J. Ceresney, Director of the SEC's Enforcement Division, explained that this "settlement demonstrates that even those beyond our borders who trade on stolen nonpublic information and use complex instruments in an attempt to avoid detection will ultimately be caught."[41] Litigation against the other thirty-two defendants is still ongoing.[42]

2. JPMorgan Cyberattack and Indictment

In July 2014, the security team at JPMorgan Chase & Co.—the largest U.S. bank—uncovered evidence of a massive cyber attack that jeopardized the contact information of over 83 million of its customers.[43] Employing rather unsophisticated hacking techniques, the hackers were able to maintain access to JP Morgan's digital network for several weeks without detection.[44] Further investigation revealed that the hacking extended beyond JP Morgan's network to

---

[35] *See* Press Release, *supra* note 32.
[36] *Id*.
[37] *Id*.
[38] Noeleen Walder et al., *7-Hackers Stole Secrets For Up to $100 Mln Insider-Trading Profit*, REUTERS (Aug. 11, 2015 9:35 PM), http://www.reuters.com/article/2015/08/12/cybersecurity-hacking-stocks-update-7-pi-idUSL1N10M05H20150812 [http://perma.cc/CGT6-Z6FL].
[39] *Id*.
[40] SEC Press Release, *supra* note 33.
[41] *Id*.
[42] *Id.*
[43] Matthew Goldstein et al., *Hackers' Attack Struck Systems at 10 Companies*, N.Y. TIMES, Oct. 4, 2014, at A1.
[44] *Id.*; Matthew Goldstein, *4 Arrested in Schemes Said to Be Tied to JPMorgan Chase Breach*, N.Y. TIMES, July 22, 2015, at B1.

include several other major financial institutions like Fidelity Investments Ltd. and E*Trade Financial Corp.[45] As stated by U.S Attorney General Loretta Lynch, the attack represented "one of the largest thefts of financial-related data in history."[46]

In July 2015, in a seemingly unrelated enforcement action, the SEC brought civil charges against Joshua Samuel Aaron, Gery Shalon, and Zvi Orenstein for taking part in an elaborate "pump-and-dump" trading scheme.[47] The men allegedly obtained large positions in numerous penny stocks, then sent "extravagantly positive promotional email[s]" about the stocks to potential investors.[48] The promotional efforts generated enough interest in the stocks to drive their prices up, but the defendants subsequently liquidated their holdings to substantial profit, leaving the hapless investors with worthless stock.[49] Prosecutors in New York also filed criminal charges against the three men.[50]

Then, in November 2015, federal authorities announced that they had arrested four individuals who were at least partly responsible for the JPMorgan cyber attacks—two of whom were Shalon and Orenstein, with Aaron deemed "at large."[51] Commenters

---

[45] Michael Riley & Jordan Robertson, *Digital Misfits Link JPMorgan Hack to Pump-and-Dump Fraud*, BLOOMBERG BUS. (July 22, 2015), http://www.bloomberg.com/news/articles/2015-07-21/fbi-israel-make-securities-fraud-arrests-tied-to-jpmorgan-hack [http://perma.cc/8MZM-UM2U].

[46] Jonathan Stempel & Nate Raymond, *U.S. Charges Three in Huge Cyberfraud Targeting JPMorgan, Others*, REUTERS (Nov. 10, 2015, 4:43 PM), http://www.reuters.com/article/2015/11/10/us-hacking-indictment-idUSKCN0SZ1VM20151110#7H505TBFPj1cdjU3.97 [http://perma.cc/5HUN-HU83].

[47] Press Release, Sec. & Exch. Comm'n, SEC Charges Three Penny Stock Promoters Behind Pump-and-Dump Schemes (July 21, 2015), *available at* http://www.sec.gov/news/pressrelease/2015-152.html [http://perma.cc/V233-AXZ3].

[48] *Id.* ("The SEC alleges that the three men . . . obtained shares in several penny stock companies and pumped the prices as high as 1,800 percent before dumping the shares for at least $2.8 million in illicit proceeds. In one extravagantly positive promotional e-mail about a particular stock, they stated that a $5,000 investment could be worth more than $250,000 in two years.").

[49] *Id.*

[50] *Id.*

[51] *See* Goldstein, *4 Arrested in Schemes Said to Be Tied to JPMorgan Chase Breach*, N.Y. TIMES, July 22, 2015, at B1.

surmised that the unlawful acquisition of customer contact information in the JPMorgan hack "may have been more of an attempt to fuel [the] ongoing pump-and-dump stock scheme rather than an effort to steal financial data," as it provided the hackers with an endless list of potential investor targets.[52] On November 10, 2015, U.S. prosecutors indicted the three men on 23 counts, citing their "lucrative securities market manipulation" scheme spanning at least four years.[53] The SEC's previously filed civil charges are still pending, but it remains to be seen whether the SEC will take any additional action in light of the new allegations.[54]

E. Guidelines to Mitigate Cybersecurity Risk

With cyber attacks amplifying in number and severity in recent years, SEC Commissioners outlined in the agency's roundtable several actions that companies should be taking to mitigate the potential harm of cyber threats.[55] These practices include:

> (i) implementing a formal written response plan separate from business continuity plans to address cybersecurity incidents and data breaches, (ii) conducting penetration tests, documenting the results, and addressing areas for improvement, (iii) risk-prioritizing sensitive data and critical infrastructure and identifying appropriate process and security controls to protect the data and infrastructure, and (iv) engaging in peer intelligence sharing, rather than viewing cybersecurity as a competitive advantage.[56]

---

[52] *Id.*
[53] Sealed Superseding Indictment at 13, U.S. v. Shalon, No. 15-cr-00333 (S.D.N.Y. filed Nov. 10, 2015), *available at* http://www.justice.gov/usao-sdny/file/792506/download [http://perma.cc/F4UW-XH3V].
[54] *See* Stempel & Raymond, *supra* note 46.
[55] *See generally Cybersecurity Roundtable*, *supra* note 3.
[56] *The SEC's Focus on Cybersecurity: Key Insights for Investment Advisors,* DELOITTE 1 (2014), http://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-the-secs-focus-on-cyber-security-070914.pdf [http://perma.cc/E6YE-YGMG].

The guidance promulgated by the SEC in April 2015 included several guidelines for registered investment companies and registered investment advisers to follow in order to improve the cybersecurity of financial firms.[57] The guidelines include: (i) periodically assessing the firm's stored information, technology systems in use, cybersecurity threats, and any potential impact of data theft, (ii) developing strategies "designed to prevent, detect and respond to cybersecurity threats," and (iii) implementing such a strategy "through written policies and procedures and training that provide guidance to officers and employees concerning applicable threats and measures to prevent, detect and respond to such threats, and that monitor compliance with cybersecurity policies and procedures."[58]

F. Regulation of Cybersecurity of Third-Party Service Providers

The hacking methods allegedly used by the defendants in *SEC v.* Dubovoy, the JPMorgan hack, and other cyber crime incidents showcase the importance of cybersecurity in an age of widespread dependence on technology.[59] Government authorities have already acknowledged cybersecurity, "especially [of third-party service providers] with access to sensitive data, as an area ripe for regulation."[60] Acknowledging the "significant potential cyber security vulnerabilities" of third-party service providers,[61] the New York State Department of Financial Services stated in an April report

---

[57] CYBERSECURITY GUIDANCE, *supra* note 14.
[58] *Id*.
[59] *See* Sigal P. Mandelker & Boris Zeldin, *SEC Brings First Major Cyber Insider Trading Case Against International Hacking Ring*, PROSKAUER ROSE LLP (Aug. 25, 2015), http://www.corporatedefensedisputes.com/2015/08/sec-brings-first-major-cyber-insider-trading-case-against-international-hacking-ring/ [http://perma.cc/4PT4-QNG2].
[60] *Id.*
[61] *See* Sigal P. Mandelker & Boris Zeldin, *Cyber Security Regulations Ahead Says New York State's Dept. of Financial Services*, PROSKAUER ROSE LLP (Apr. 19, 2015), http://www.corporatedefensedisputes.com/2015/04/cyber-security-regulations-ahead-says-new-york-states-dept-of-financial-services/ [http://perma.cc/3T3Z-L2AG].

that it was considering imposing regulatory requirements on financial institutions in connection to any relationships they maintain with these third parties.[62] The Financial Industry Regulatory Authority recommends performing "risk-based due diligence" on the cybersecurity practices of prospective third party service providers.[63] In February 2015, the SEC released a "Risk Alert" that outlined cybersecurity concerns facing brokerage and advisory firms.[64] This Risk Alert found that "[m]any firms failed to require vendors to conduct adequate cybersecurity assessments because they did not incorporate security requirements into agreements with vendors."[65]

For a cybersecurity program to be optimally effective, it should not contain any weak links that are exploitable by hackers.[66] In *SEC v. Dubovoy*, the hackers breached the security of third-party newswires, rather than the companies that created the information.[67] The newswires' servers contained a plethora of nonpublic information about hundreds of publicly traded companies.[68] The hackers were likely able to obtain this information because the newswires "may have . . . presented a weak link by having weaker cybersecurity measures than the public companies themselves."[69] *SEC v. Dubovoy* may signal a shift by companies from relying on

---

[62] NEW YORK STATE DEP'T OF FIN. SERVS., UPDATE ON CYBER SECURITY IN THE BANKING SECTOR: THIRD PARTY SERVICE PROVIDERS (2015).

[63] *See* FIN. REGULATORY AUTH., REPORT ON CYBERSECURITY PRACTICES (2015), *available at* https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf [http://perma.cc/X69R-B4UB].

[64] *International Hacking and Insider Trading Scheme Exposes Cybersecurity Vulnerabilities at Third-Party Vendors*, ORRICK, HERRINGTON & SUTCLIFFE 1 (Aug. 20, 2015), https://www.orrick.com/Events-and-Publications/Pages/International-Hacking-and-Insider-Trading-Scheme-Exposes-Cybersecurity-Vulnerabilities-at-Third-Party-Vendors.aspx [http://perma.cc/V7CJ-XZTL].

[65] *Id.*

[66] *SEC and DOJ Hacking Prosecutions Highlight SEC's Increased Interest in Cybersecurity Risks*, MORGAN LEWIS & BOCKIUS LLP 1 (Sep. 15, 2015), http://www.morganlewis.com/pubs/sec-and-doj-hacking-prosecutions-highlight-secs-increased-interest-in-cybersecurity-risks [http://perma.cc/53D3-Y26U] [hereinafter *SEC and DOJ Hacking Prosecutions*].

[67] *Id*.

[68] *See* SEC Press Release, *supra* note 32.

[69] *See SEC and DOJ Hacking Prosecutions*, *supra* note 66.

newswires to communicate earnings data to instead utilizing their own online platforms.[70] Many large companies, such as Google, Microsoft, and Tesla already release sensitive information on their own and thus without the use of newswires.[71]

E. Conclusion

Illegal trading was once limited to the "'insiders' in the financial markets."[72] These traditional insiders tended to operate on a more interpersonal level; they were "connected to key facts and secrets [and] passed information to golf buddies, drinking buddies, friends, or relatives."[73] Consequently, the SEC has attempted to deal with illegal insider trading by "improv[ing] systems integrity for certain key market participants."[74] Prosecutors have been using tactics such as wiretaps to discover illegal trading, but if criminals are stealing the information without cooperating with an "insider," these tactics will be ineffective.[75] The advent of digital technology and its corresponding vulnerabilities has complicated the insider trading dynamic, as regulators now have to attempt to police data theft in the cyber realm, despite regulatory infrastructure only designed to uncover securities fraud in its more established communication-based forms.[76] Yet the abundant risks deriving from cyber crime that have become increasingly visible in recent years will likely require a heightened focus from regulators in order to effectively safeguard our economic security.[77]

---

[70] *See* Noeleen Walder et al., *supra* note 38.
[71] *Id.*
[72] Kara M. Stein, Commissioner, Sec. & Exch. Comm'n, Accountants and Capital Markets in an Era of Digital Disruption: Remarks to the Institute of Chartered Accountants in England and Wales and BritishAmerican Business (Sept. 9, 2015), *available at* http://www.sec.gov/news/speech/remarks-inst-chartered-acctnts.html [http://perma.cc/MR23-6ELA].
[73] *Id*.
[74] *Id*.
[75] *See* Keri Geiger, *U.S. Identifies Insider Trading Ring With Ukraine Hackers*, BLOOMBERG BUS. (Aug. 11, 2015, 5:59 PM) http://www.bloomberg.com/news/articles/2015-08-11/u-s-identifies-insider-trading-ring-including-ukraine-hackers [http://perma.cc/2CP7-N3SK].
[76] *See id.*
[77] *See generally Cybersecurity Roundtable*, *supra* note 3.

Matthew B. Hilowitz[78]

[78] Student, Boston University School of Law (J.D. 2017).