Boston College Law Review

Volume 61 | Issue 4 Article 7

4-30-2020

From Securities to Cybersecurity: The SEC Zeroes In on Cybersecurity

Rebecca Rabinowitz
Boston College Law School, rebecca.rabinowitz@bc.edu

FROM SECURITIES TO CYBERSECURITY: THE SEC ZEROES IN ON CYBERSECURITY

Abstract: Cybersecurity is one of the gravest threats facing public companies, the markets, and the economy at large today. Because of this pressing threat, the SEC has increased its attention to cybersecurity. In 2018 interpretive guidance, consistent with the mandatory disclosure regime established by federal securities regulation, the SEC stipulated that public companies have a duty to disclose those cybersecurity risks and incidents that are material to investors. The 2018 guidance added little, however, and instead parroted earlier guidance from the SEC's Division of Corporation Finance. Moreover, the SEC itself has been plagued by cybersecurity problems. This Note asserts that to regulate cybersecurity effectively, the SEC must both strengthen its own cybersecurity and further expand upon, rather than simply repeat, the obligation of public companies to disclose cybersecurity risks and incidents.

INTRODUCTION

On November 30, 2018, Marriott International, Inc. ("Marriott"), the largest hotel company in the world, publicly disclosed a breach of its Starwood guest reservation database in a Current Report on Form 8-K filed with the United States Securities and Exchange Commission (SEC or the "Commission").[1] Marriott revealed that the cybersecurity incident, which implicated the sensitive personal information of nearly four hundred million guests, dated to September 2014.[2] The Marriott cybersecurity incident was one of the largest in

[1] Marriott Int'l, Inc., Current Report (Form 8-K) (Nov. 30, 2018); Francine McKenna, *Marriott's Starwood Breach Raises Questions About Meeting SEC Standards for Cybersecurity Disclosure*, MARKETWATCH (Nov. 30, 2018), https://www.marketwatch.com/story/Marriotts-starwood-breach-raises-questions-about-meeting-sec-standards-for-cybersecurity-disclosure-2018-11-30 [https://perma.cc/S8W7-ZAPF]. Guests of Starwood Hotels & Resorts Worldwide, Inc. ("Starwood") properties input sensitive personal information into the Starwood guest reservation system to secure their reservations at Marriott properties. *See* Marriott Int'l, Inc., Exhibit 99 to Current Report (Form 8-K) (Nov. 30, 2018) (noting that the Starwood reservation database houses Starwood guests' personal information). Pursuant to the mandatory disclosure regime implemented by the federal securities laws, public companies are required to file a Current Report on Form 8-K with the SEC to report the existence of certain material events, such as amendments to governance documents, entry into certain material agreements, or voting results from the annual meeting of the shareholders. *Fast Answers: Form 8-K*, U.S. SEC. & EXCHANGE COMMISSION, https://www.sec.gov/fast-answers/answersform8k htm.html [https://perma.cc/FRG3-UG9F]; *see* 17 C.F.R. § 249.308 (2020) (explaining that the Form 8-K is to be filed pursuant to a company's disclosure obligations under the Securities Exchange Act of 1934).

[2] McKenna, *supra* note 1; *Marriott Provides Update on Starwood Database Security Incident*, MARRIOTT INT'L NEWS CTR. (Jan. 4, 2019), http://news.Marriott.com/2019/01/Marriott-provides-update-on-starwood-database-security-incident [https://perma.cc/32BA-9DQ4]. Marriott revealed that

history, exceeded only by the mammoth breach of Yahoo! Inc. ("Yahoo!") in 2013 and 2014.[3] Marriott and Yahoo! are not alone in facing the cybersecurity threat; it is one of the most pressing concerns in corporate boardrooms around the world.[4]

Marriott's eventual disclosure of the Starwood breach has strong implications for recent SEC guidance regarding cybersecurity-related disclosures.[5] Although it learned of the breach in September 2018, Marriott did not disclose

---

in September 2018 it learned that unsanctioned access to the Starwood network enabled an unapproved user to access and copy encrypted user information. Marriott Int'l, Inc., Exhibit 99 to Current Report (Form 8-K) (Nov. 30, 2018). Some of the personal information implicated included guest names, dates of birth, passport numbers, and payment information. *Id.* The hackers gained access to the system in 2014, although Marriott only learned of the breach in 2018, two years after its acquisition of Starwood. McKenna, *supra* note 1; *see Marriott International to Acquire Starwood Hotels & Resorts Worldwide, Creating the World's Largest Hotel Company*, MARRIOTT BONVOY (Nov. 16, 2015), https://marriott.gcs-web.com/news-releases/news-release-details/marriott-international-acquire-starwood-hotels-resorts-worldwide [https://perma.cc/7R4D-8HGY] (announcing the transaction between Marriott and Starwood, and indicating its expected closing in the middle of 2016).

[3] Kirsten Grind & Dustin Volz, *Marriott Says Hackers Swiped Millions of Passport Numbers*, WALL ST. J. (Jan. 4, 2019), https://www.wsj.com/articles/Marriott-says-hackers-swiped-millions-of-passport-numbers-11546605000/?mod=mktw [https://perma.cc/NW2F-36YK]. The breach of Yahoo! implicated more than one billion accounts. William Pierotti, *Cyber Babel: Finding the Lingua Franca in Cybersecurity Regulation*, 87 FORDHAM L. REV. 405, 406 (2018). At the time Yahoo! disclosed the breaches, it was in talks to be acquired by Verizon Communications Inc. ("Verizon"). *See id.* (describing the effect of the breach on Verizon's eventual acquisition of Yahoo!). Because of the Yahoo! breaches, Verizon reduced its suggested purchase price from $4.83 billion to $4.48 billion. *Id.* (noting that the $350 million decrease represented a seven percent reduction in purchase price). For further discussion of the Yahoo! breach and subsequent SEC enforcement action, see *infra* notes 137–141 and accompanying text.

[4] *See* Chenxi Wang, *Corporate Boards Are Snatching Up Cybersecurity Talents*, FORBES (Aug. 30, 2019), https://www.forbes.com/sites/chenxiwang/2019/08/30/corporate-boards-are-snatching-up-cybersecurity-talents/#29cfbdb5479f [https://perma.cc/8JTQ-3YB4] (noting that corporate boards are shoring up their cybersecurity governance and expertise in response to the growing threat of cybersecurity incidents and pressure from investors); *Business E-Mail Compromise: The 12 Billion Dollar Scam*, FED. BUREAU INVESTIGATION (July 12, 2018), https://www.ic3.gov/media/2018/180712.aspx [https://perma.cc/9X2H-XFKC] (noting that more than seventy-eight thousand "business e-mail compromises" have caused more than $12.5 billion in fraud losses since 2013). The "business e-mail compromise" is a scam targeting companies that conduct payments via wire transfer. *Business E-Mail Compromise: The 12 Billion Dollar Scam*, *supra*. Moreover, businesses are not the only affected parties; individual users are similarly affected. *See id.* (identifying more than forty thousand individual victims of "business e-mail compromise" scams).

[5] McKenna, *supra* note 1. The delay between when the breaches occurred and Marriott's eventual disclosure of the breaches raises questions about the timeliness of the disclosure under the SEC's new guidance. *See id.* (questioning whether Marriott informed investors of the cybersecurity incidents in a timely manner); *see also* Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Exchange Act Release No. 33-10459, 83 Fed. Reg. 8166, 8167 (Feb. 26, 2018) (articulating the SEC's position that public companies are obligated to disclose cybersecurity risk of material significance to their investors in a "timely fashion"). Although the SEC reinforced the need for timely disclosure of cybersecurity risks, it did not expound on what makes disclosure "timely." *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. at 8167 (providing only that companies must endeavor to provide timely disclosure).

the breach in filings with the SEC until the end of November 2018, raising questions as to whether the disclosure was timely under the SEC guidance.[6]

Federal securities regulation encompasses twin pursuits: the regulation of securities exchanges and investor protection.[7] These pursuits underlie the statutory framework of securities regulations, established principally by the Securities Act of 1933 ("Securities Act") and the Securities Exchange Act of 1934 ("Exchange Act" and, together, the "Acts").[8] Pursuant to the authority granted to the Commission to regulate the securities industry, the SEC has developed a regulatory framework predicated on mandatory disclosure.[9] Although its efficacy is debated, disclosure is thought to promote market efficiency and ensure a well-informed investing population.[10]

---

[6] *See* Marriott Int'l, Inc., Exhibit 99 to Current Report (Form 8-K) (Nov. 30, 2018) (disclosing at the end of November 2018 the existence of a massive breach to the Starwood reservation database to which the company was alerted on September 8, 2018); Shivaram Rajgopal & Bugra Gezer, *The Marriott Breach Shows Just How Inadequate Cyber Risk Disclosures Are*, HARV. BUS. REV. (Mar. 5, 2019), https://hbr.org/2019/03/the-marriott-breach-shows-just-how-inadequate-cyber-risk-disclosures-are [https://perma.cc/T4DV-4D5B] (arguing that a lack of definition of "timely" in the SEC's guidance on cybersecurity disclosure enabled the delay in Marriott's disclosure of its breach to the SEC and investors). Significant litigation ensued: On January 11, 2019, 176 plaintiffs from across the United States initiated class action proceedings in Maryland federal court. Joyce Hanson, *Marriott Hit with Another Suit Over Starwood Data Breach*, LAW360 (Jan. 30, 2019), https://www.law360.com/articles/1123696/marriott-hit-with-another-suit-over-starwood-data-breach [https://perma.cc/2QH7-6QLQ]; *see also* Dave Simpson, *11 Marriott Data Breach Suits Moved to Maryland for MDL*, LAW360 (Feb. 6, 2019), https://www.law360.com/articles/1126573/11-marriott-data-breach-suits-moved-to-maryland-for-mdl [https://perma.cc/669T-KFU7] (describing the complexity of the judicial proceedings).

[7] *See* Chadbourne & Parke LLP v. Troice, 571 U.S. 377, 390 (2014) (noting that the federal securities laws aim to protect investors by ridding the exchanges of abusive misconduct).

[8] Securities Exchange Act of 1934, ch. 404, 48 Stat. 881 (codified as amended at 15 U.S.C. §§ 78a–78qq (2018)); Securities Act of 1933, ch. 38, 48 Stat. 74 (codified as amended at 15 U.S.C. §§ 77a–77aa); Blue Chip Stamps v. Manor Drug Stores, 421 U.S. 723, 728–29 (1975) (describing the history and purpose of the Acts). The purpose of the Securities Act was to ensure complete and accurate disclosure of securities offered for sale in interstate commerce and to protect against abusive behavior. *Blue Chip Stamps*, 421 U.S. at 728. The Exchange Act purported both to regulate and protect against abusive practices in the securities exchanges and over-the-counter (OTC) trading markets operating in interstate commerce. *Id.*

[9] *See Blue Chip Stamps*, 421 U.S. at 728–29 (noting that Section 4(a) of the Exchange Act created the SEC); John C. Coffee, Jr., *Market Failure and the Economic Case for a Mandatory Disclosure System*, 70 VA. L. REV. 717, 723 (1984) (identifying mandatory disclosure as the original premise upon which federal securities regulation was predicated). Mandatory disclosure seeks to ensure that SEC issuers provide investors with all material information pertaining to their investments. Daniel M. Gallagher, Comm'r, U.S. Sec. & Exch. Comm'n, Remarks at Society of Corporate Secretaries & Governance Professionals (July 11, 2013), https://www.sec.gov/news/speech/spch071113dmghtm [https://perma.cc/3CCW-N2WJ] (noting that the premise of the mandatory disclosure regime is to enable investors to make intelligent investment decisions).

[10] *See* Lauren M. Mastronardi, Note, *Shining the Light a Little Brighter: Should Item 303 Serve as a Basis for Liability Under Rule 10b-5?*, 85 FORDHAM L. REV. 335, 343 (2016) (describing why disclosure is utilized in the securities regulation context and highlighting the debate over its efficacy). Mandatory disclosure improves efficiency in the market because increasing the market's supply of accurate information ensures that investors are best situated to make informed decisions about invest-

Recently, the SEC has begun to focus its regulatory efforts on cybersecurity, recognizing that it is of concern to all companies in its regulatory jurisdiction, regardless of industry or type of entity.[11] In 2011, the SEC's Division of Corporation Finance issued guidance pertaining to the disclosure of cybersecurity risks and incidents in SEC filings.[12] The 2011 guidance did not generate any new reporting obligations, but rather reaffirmed public companies' obligation to disclose material information to their investors, which may include cybersecurity risks and incidents.[13] In February 2018, the SEC issued interpretive guidance pertaining to the disclosure obligations of companies that it regulates with respect to cybersecurity risks and incidents.[14] The 2018 guidance further developed the Division of Corporation Finance's 2011 guidance.[15]

Some critics of this approach argue that the SEC should go beyond the mandatory disclosure regime to regulate cybersecurity through more proactive means, whereas others recognize that cybersecurity risks and incidents are critical information about which investors need to be informed.[16] Although the

---

ment opportunities. Frank H. Easterbrook & Daniel R. Fischel, *Mandatory Disclosure and the Protection of Investors*, 70 VA. L. REV. 669, 673 (1984).

[11] *See* Jay Clayton, Chairman, U.S. Sec. & Exch. Comm'n, Statement on Cybersecurity (Sept. 20, 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20 [https://perma.cc/V7J3-S4PC] (emphasizing the SEC's commitment to regulating "cybersecurity risks and incidents" and taking care that market participants are adequately informed regarding such risks and incidents).

[12] *See* Div. of Corp. Fin., *CF Disclosure Guidance: Topic No. 2: Cybersecurity*, U.S. SEC. & EXCHANGE COMMISSION (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm [https://perma.cc/78WD-S6D9] (outlining the cybersecurity disclosure requirements developed by the SEC's Division of Corporation Finance). The Division of Corporation Finance works to equip investors with "material information in order to make informed investment decisions." *About the Division of Corporation Finance*, U.S. SEC. & EXCHANGE COMMISSION, https://www.sec.gov/divisions/corpfin/cfabout.shtml [https://perma.cc/5UME-8X3N]. In pursuit of this goal, the Division reviews select filings with the SEC and issues interpretative guidance regarding SEC rules and form. *Id.*

[13] *See* Loren F. Selznick & Carolyn LaMacchia, *Cybersecurity: Should the SEC Be Sticking Its Nose Under This Tent?*, 2016 U. ILL. J.L. TECH. & POL'Y 35, 45–49 (describing the content and implications of the 2011 guidance). The guidance was issued by the SEC's Division of Corporation Finance, but it did not have the force of law. *See id.* at 46 & n.96 (noting that the 2011 guidance was not issued by the SEC through the notice and comment procedures required to promulgate a regulation); *infra* note 16 and accompanying text.

[14] *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosure, 83 Fed. Reg. at 8167 (discussing guidance updates to the cybersecurity disclosure requirements articulated by the SEC's Division of Corporation Finance in 2011).

[15] *See id.* (noting that the 2018 guidance "reinforc[es] and expand[s]" on the Division of Corporation Finance's 2011 guidance).

[16] *See* Kara M. Stein, Comm'r, U.S. Sec. & Exch. Comm'n, Statement on Commission Statement and Guidance on Public Company Cybersecurity Disclosures (Feb. 21, 2018), https://www.sec.gov/news/public-statement/statement-stein-2018-02-21#_ednref1 [https://perma.cc/UG3Q-JKHJ] (suggesting that the SEC should go further than simply requiring disclosure); *see also* Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. at 8171 (describing disclosure controls and procedures that the SEC believes public companies should adopt). Former SEC Commissioner Kara Stein proposed pursuing notice and comment rulemaking on more proactive

SEC has confirmed that disclosure obligations imposed on entities regulated by the SEC include disclosure of cybersecurity incidents, the Commission's 2018 guidance merely repeats, rather than further develops, a public company's disclosure obligations.[17] The more recent guidance also underestimates the difficulty in providing this disclosure without compromising sensitive corporate information, a challenge that is compounded by the SEC's own cybersecurity challenges.[18]

Part I of this Note discusses the history of federal securities regulation, the history of and disclosure requirements related to the SEC's regulation of cybersecurity, and the underlying rationale of the mandatory disclosure regime.[19] Part II of this Note addresses the implications of the SEC's regulation of cybersecurity, and considers whether the SEC should be regulating in this space, and if so, whether mandatory disclosure is the most effective means by which the SEC can assert oversight.[20] Finally, Part III of this Note argues that although the SEC has rightly chosen to regulate cybersecurity, to be effective

---

cybersecurity measures, such as minimum standards that SEC-regulated entities should abide by to protect sensitive consumer information. Stein, *supra*. Notice and comment is part of the procedure by which the SEC, in addition to other federal agencies, exercises its rulemaking authority. *Investor Bulletin: Suggestions for How Individual Investors Can Comment on SEC Rulemaking*, U.S. SEC. & EXCHANGE COMMISSION (Dec. 12, 2017), https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_secrulemaking [https://perma.cc/2JQU-3V66]. Before promulgating final rules, the SEC will publish a notice with a proposal for a rule and will subsequently seek comment from the public. *Id.* Members of the public likely to provide comments include individual investors, law firms, and regulated entities, among others. *See SEC Proposed Rules*, U.S. SEC. & EXCHANGE COMMISSION, https://www.sec.gov/rules/proposed.shtml [https://perma.cc/D6WB-FJXU] (making available a list of proposed rules considered by the SEC, as well as comments received for proposed rules whose comment period has closed). The SEC considers the public comments and then promulgates the final version of the rule. *Investor Bulletin: Suggestions for How Individual Investors Can Comment on SEC Rulemaking*, *supra*.

[17] *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosure, 83 Fed. Reg. at 8168–69 (noting that the companies must disclose material information pertaining to cybersecurity incidents, but need not include sensitive corporate information in such disclosures). Along with the disclosure content explicitly mandated by SEC regulations, public companies must disclose all "material information" necessary to ensure that the statements being made are not misleading. 17 C.F.R. § 240.12b-20. Consistent with the United States Supreme Court, the SEC considers information to be material if it is substantially likely that a reasonable investor would view the information as important to her investment decision, or if the reasonable investor would have considered disclosure of the information as having substantially changed the total volume of information available to him or her. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. at 8168 (citing TSC Indus., Inc. v. Northway, 426 U.S. 438, 449 (1976)).

[18] *See* Steve W. Klemash et al., *Cybersecurity Disclosure Benchmarking*, HARV. L. SCH. F. ON CORP. GOVERNANCE & FIN. REG. (Oct. 21, 2018), https://corpgov.law.harvard.edu/2018/10/21/cybersecurity-disclosure-benchmarking/ [https://perma.cc/398N-SW25] (noting the difficulties faced by issuers in providing adequate disclosure while also not revealing sensitive information that could make its way to nefarious parties). For a discussion of the 2016 breach of an SEC database, see *infra* note 119 and accompanying text.

[19] *See infra* notes 22–141 and accompanying text.

[20] *See infra* notes 142–187 and accompanying text.

in its efforts it must further clarify the substance and timing of disclosures of cybersecurity risks and incidents as well as shore up its own cybersecurity.[21]

I. SEC Regulation: Where It Has Been and Where It Is Going

Federal regulation of securities emerged in response to the Great Depression.[22] Through the Securities Act and the Exchange Act, the SEC has established a regulatory regime predicated upon mandatory disclosure.[23] Since the initial enactment of the federal securities laws in the early twentieth century, the SEC has further developed this regulatory scheme.[24] Section A of this Part traces the history of federal securities regulation in the United States.[25] Section B of this Part presents the underlying rationale of mandatory disclosure, the regime upon which federal securities regulation is premised.[26] Section C details the regulation of cybersecurity by the SEC.[27]

A. The 1929 Stock Market Crash Leads to the Establishment of Federal Securities Regulation

Before the Great Depression, the federal government had little involvement in the regulation of the securities markets.[28] Following the 1929 stock

---

[21] *See infra* notes 188–215 and accompanying text.

[22] *See, e.g.*, Kokesh v. SEC, 137 S. Ct. 1635, 1639–40 (2017) (describing the initiation of federal securities regulation in the United States and noting that the "rampant abuses" in securities exchanges that caused the 1929 stock market crash pushed Congress to enact the federal securities laws). *See generally* Elisabeth Keller & Gregory A. Gehlmann, *Introductory Comment: A Historical Introduction to the Securities Act of 1933 and the Securities Exchange Act of 1934*, 49 Ohio St. L.J. 329 (1988). For a more detailed description of the initial enactment of the federal securities laws, see *infra* notes 28–33 and accompany text.

[23] *See* Securities Exchange Act of 1934 (requiring continuous disclosure after the initial public offering of securities to the market); Securities Act of 1933 (requiring disclosure upon the initial public offering of securities); Mastronardi, *supra* note 10, at 336 (noting that securities regulation was premised upon disclosure from the outset).

[24] *See, e.g.*, Adoption of the Integrated Disclosure System, Exchange Act Release No. 18,524, 47 Fed. Reg. 11,380, 11,380 (Mar. 16, 1982) (adopting a scheme of integrated disclosure to eliminate redundancies in the reporting obligations under the Securities Act of 1933 and the Securities Exchange Act of 1934). For a detailed discussion of the SEC's adoption of an integrated disclosure scheme, see *infra* notes 64–73 and accompanying text.

[25] *See infra* notes 28–73 and accompanying text.

[26] *See infra* notes 74–83 and accompanying text.

[27] *See infra* notes 84–141 and accompanying text.

[28] *See* Robert B. Thompson & Hillary A. Sale, *Securities Fraud as Corporate Governance: Reflections upon Federalism*, 56 Vand. L. Rev. 859, 869 (2003) (describing President Theodore Roosevelt's call for stronger regulation of corporations); *What We Do*, U.S. Sec. & Exchange Commission, https://www.sec.gov/Article/whatwedo.html [https://perma.cc/FG4A-ZVP6] (noting that in the period before the Great Depression there was negligible federal oversight of the securities markets in the United States). Although President Theodore Roosevelt's call for federal regulation was reiterated by two later presidents, Congress did not enact any federal legislation until the Great Depression. Thompson & Sale, *supra*, at 869. Moreover, the period between World War I and the Great Depres-

market crash, Congress adduced that one of the crash's primary causes was abusive market conduct.[29] Consequently, in reforming the market, one of Congress's principal goals was to protect lay investors who were susceptible to such abuse.[30] Its second priority was to ensure the integrity of the securities exchanges.[31] As part of the New Deal legislation, Congress enacted the princi-

---

sion experienced prolific economic participation and many individual investors entered the market for the first time. Allison Grey Anderson, *The Disclosure Process in Federal Securities Regulation: A Brief Review*, 25 HASTINGS L.J. 311, 316 (1974). A larger population of investors and a resulting higher demand for securities led to elevated stock prices. *Id.* Approximately fifty billion dollars in new securities were offered during this period; half became worthless due to the 1929 stock market crash. H.R. REP. NO. 73-85, at 2 (1933); *see also What We Do*, *supra* (summarizing the historical events that led to the establishment of federal securities regulation). The 1929 stock market crash initiated the Great Depression, a period of deep economic recession in the United States that lasted late into the 1930s. *See* Joy Sabino Mullane, *Perfect Storms: Congressional Regulation of Executive Compensation*, 57 VILL. L. REV. 589, 594 (2012) (describing the Great Depression and noting that unemployment in this period peaked at 24.9% in 1933). Prior to the Great Depression, securities were regulated at the state level by so-called "blue sky" laws. *See* Eric C. Chaffee, *Securities Regulation in Virtual Space*, 74 WASH. & LEE L. REV. 1387, 1401–02 (2017) (noting that Kansas passed the first securities law in 1911, with many other jurisdictions following suit over the subsequent two decades); Keller & Gehlmann, *supra* note 22, at 331 (quoting MICHAEL E. PARRISH, SECURITIES REGULATION AND THE NEW DEAL 5 n.1 (1970)) (explaining that the "blue sky" laws were so named because lawmakers posited that, without intervention, "financial pirates would sell citizens everything in [the] state *but* the blue sky"). The securities industry's principal participants had persuaded state legislatures to adopt schemes of self-regulation. *See* Anderson, *supra*, at 318 (noting that the self-regulation scheme perpetuated by state statutes constituted an ineffective means of securities regulation). Unsurprisingly, the resulting hodgepodge of state statutes was too varied to be effective. *See* Chaffee, *supra*, at 1402 (asserting that various state securities statutes ultimately contributed to the stock market crash and the ensuing depression). *See generally* Jonathan R. Macey & Geoffrey P. Miller, *Origin of the Blue Sky Laws*, 70 TEX. L. REV. 347 (1991) (describing the history of state blue sky laws).

[29] *See* Mastronardi, *supra* note 10, at 339 (explaining how abusive practices, such as malicious price manipulation, contributed to the crash). During the depression that followed the crash, investors' funds were wiped out and the public's confidence in the securities exchanges declined. *What We Do*, *supra* note 28. Post-crash Senate hearings evidenced the fraudulent conduct that operated on the securities exchanges during the 1920s and early 1930s, such as price manipulation and self-dealing. Anderson, *supra* note 28, at 316–17 (citing *Stock Exchange Practices: Hearings on S. Res. 84 and S. Res. 56 Before the S. Comm. on Banking & Currency*, 72d and 73d Congs. (1932–1934)). For example, wrongful manipulation occurred when professionals working within the New York Stock Exchange orchestrated fluctuations in stock prices either to encourage the public to buy—and thereby allow the professionals to unload their holdings—by creating high prices, or to induce it to sell by depressing the prices. Steven Thel, *The Original Conception of Section 10(b) of the Securities Exchange Act*, 42 STAN. L. REV. 385, 399 (1990). The lack of regulation allowed these abusive practices to perpetuate and ultimately exploited the unsuspecting public, comprised of unsophisticated individual investors in the exchanges. Anderson, *supra* note 28, at 317.

[30] Mastronardi, *supra* note 10, at 339; *see Chadbourne & Parke*, 571 U.S. at 390 (stating that federal securities law aims to protect the exchanges from abusive behavior and thus protect investors); Anderson, *supra* note 28, at 316 (describing an investing public that, prior to the 1929 stock market crash, was not well situated to protect itself against abusive market conduct).

[31] *See* Securities Exchange Act of 1934 (identifying the purpose of the act as regulating the exchanges and OTC markets). Requiring issuers to provide accurate disclosure of certain required information ensures the integrity of the markets. Thompson & Sale, *supra* note 28, at 909. Moreover, some contend that the primary benefit of the disclosure regime is to provide more accurate assess-

pal vehicles of federal securities legislation: the Securities Act and the Exchange Act.[32] Operating in tandem, the Acts created a system of federal securities regulation premised upon mandatory disclosure.[33]

---

ments of a security's worth. Anderson, *supra* note 28, at 320. Stated differently, the market benefits from having prices better reflect the worth of the underlying securities. *See id.* at 320–21 (noting that modern scholars argue that investor protection was a secondary result of the mandatory disclosure regime).

[32] Securities Exchange Act of 1934; Securities Act of 1933; *Blue Chip Stamps*, 421 U.S. at 727–28; Thompson & Sale, *supra* note 28, at 869. Together, the dual aims of the Acts are to regulate the exchanges and to protect investors. *See* Matthew C. Turk & Karen E. Woody, *The* Leidos *Mixup and the Misunderstood Duty to Disclose in Securities Law*, 75 WASH. & LEE L. REV. 957, 968 (2018) (pointing to investor protection and capital formation as the "twin goals" of federal securities regulation). The mandatory disclosure regime seeks to further these purposes by ensuring investors are positioned to make fully informed investment decisions. *Id.* at 968–69. Lawmakers, however, had contemplated various schemes by which to achieve securities reform. *See* Thompson & Sale, *supra* note 28, at 869 (discussing the various schemes contemplated for federal securities legislation). Where others advocated for a system built upon direct government supervision, President Franklin Delano Roosevelt contemplated a system premised upon disclosure. Mastronardi, *supra* note 10, at 339. Invasive methods of government regulation were considered. *See id.* (noting that legislative response to the Great Depression included calls for a federal corporations law). The disclosure regime, however, ultimately carried the day. *See* Turk & Woody, *supra*, at 969 (describing the regulatory framework created by the Acts as one based upon a system of mandatory disclosure).

[33] *See* Anderson, *supra* note 28, at 320–21 (describing the effect of the Acts and noting that they both employ mandatory disclosure as the means to prevent abusive behavior). Under the system created by the Acts, public companies are required to disclose certain important information to investors via various documents filed with the SEC. *What We Do*, *supra* note 28. The most typical forms of disclosure documents are Annual Reports on Form 10-K, Quarterly Reports on Form 10-Q, and Current Reports on Form 8-K. *See infra* note 47 and accompanying text. Mandatory disclosure is thought to create efficiency in the markets by decreasing information asymmetry between issuers and investors, and in so doing, avoiding costly, more intrusive forms of regulation. Turk & Woody, *supra* note 32, at 969 n.49. Making information available to the market ensures capital goes to its highest and best use. *See* Alicia J. Davis, *Market Efficiency and the Problem of Retail Flight*, 20 STAN. J.L. BUS. & FIN. 36, 45–46 (2014) ("If prices reflect informed judgments by market investors, stock prices are tools to help ensure that the companies that are the most profitable or efficient at providing desired goods and services receive the greatest share of investment capital."). The book *The Modern Corporation and Private Property*, authored by Adolf A. Berle and Gardiner C. Means, greatly influenced the drafters of the federal securities laws. Turk & Woody, *supra* note 32, at 969 n.52. The work contended that management must answer to shareholders through the mandatory disclosure regime. *Id.* Louis Brandeis offered a frequently-quoted justification for mandatory disclosure when he remarked, "'[s]unlight is said to be the best of disinfectants; electric light the most efficient policeman.'" *Id.* (quoting LOUIS D. BRANDEIS, OTHER PEOPLE'S MONEY AND HOW THE BANKERS USE IT 92 (1914)). Stated differently, compelling issuers to provide truthful information to the public can deter abusive conduct. *See* Cary Martin Shelby, *Closing the Hedge Fund Loophole: The SEC as the Primary Regulator of Systemic Risk*, 58 B.C. L. REV. 639, 653 (2017) ("In other words, broadcasting information to large audiences can serve to uncover malfeasance and bad behavior."). Mandatory disclosure ensures that investors are well-situated to make informed investing decisions and thus are less susceptible to abusive market practices. Troy A. Paredes, Comm'r, U.S. Sec. & Exch. Comm'n, Remarks Before the Symposium on "The Past, Present, and Future of the SEC" (Oct. 16, 2009), https://www.sec.gov/news/speech/2009/spch101609tap.htm [https://perma.cc/FFR6-GYJ7].

1. The Securities Act of 1933

The Securities Act governs the initial public offering of new securities to the market, examining these issuances through a transactional lens.[34] To correct the information-asymmetry inherent in the initial public offering, the law requires detailed disclosures to accompany the offering.[35] Under the Securities Act, in the absence of an applicable exemption, no security can be offered for sale in interstate commerce without the issuer first filing a registration statement with the SEC.[36] Although the specific disclosure obligations vary among industries, a registration statement typically must thoroughly describe the issuer's business, management, and nature of the securities offered and must provide copious financial information.[37]

Notably, the Securities Act does not bestow authority on the SEC to evaluate the securities being registered.[38] Although the Securities Act imposes a twenty-day waiting period between a registration statement's date of filing and its date of effectiveness, the registration statement automatically becomes effective so long as its contents are not misleading or inadequate.[39] The issuer

---

[34] Thompson & Sale, *supra* note 28, at 869; Turk & Woody, *supra* note 32, at 969 (citing 15 U.S.C. § 77a); *see* Barbara Ann Banoff, *Regulatory Subsidies, Efficient Markets, and Shelf Registration: An Analysis of Rule 415*, 70 VA. L. REV. 135, 137 (1984) (describing the transactional disclosure requirements implemented by the Securities Act, which obligate an issuer to file a registration statement with the SEC prior to selling its securities). Some consider the initial public offering (IPO) to be the most important instance of information asymmetry sought to be remedied by the federal securities laws because in the IPO an issuer sells securities to outside parties who presumably know next to nothing about the issuer. Thompson & Sale, *supra* note 28, at 869. Without mandatory disclosure, the investors are left in the dark with respect to the issuer's business operations and financial outlook, among other things. *See id.*

[35] *See* Anderson, *supra* note 28, at 323 (describing some of the detailed information required to be divulged in the registration statement for an IPO); Thompson & Sale, *supra* note 28, at 869–70 (noting that IPOs involve a company offering securities for sale to individuals who are largely uninformed about the issuer's operations and financial situation and who have no way to get such information).

[36] Anderson, *supra* note 28, at 321; Mastronardi, *supra* note 10, at 339. Prior to the enactment of the Exchange Act, the statute that created the SEC, the Federal Trade Commission administered the Securities Act. JAMES D. COX ET AL., SECURITIES REGULATION 14 (8th ed. 2017). Exemptions from the registration statement requirement include transactions involving certain forms of securities or securities in specific types of transactions. Anderson, *supra* note 28, at 321 n.49 (citing the Securities Act of 1933 §§ 3, 4, 15 U.S.C. §§ 77c, 77d). For example, Section 3 of the Securities Act exempts securities issued by banks, insurance companies, and government entities. Securities Act of 1933 § 3, 15 U.S.C. § 77c.

[37] COX ET AL., *supra* note 36, at 6.

[38] *See* Anderson, *supra* note 28, at 322 (noting the Securities Act did not empower the SEC to assess the quality of securities an issuer offered for sale). Furthermore, the Securities Act criminalized the act of representing that the SEC made any assessment as to a security's value or worth. *Id.* at 322 n.50 (citing Securities Act of 1933 § 23, 15 U.S.C. § 77w). Thus, the SEC had little oversight as to the content of an issuer's registration statement. *See id.* at 322 (describing the lack of substantive authority the SEC possessed under the Securities Act).

[39] *See id.* (citing Securities Act of 1933 § 8, 15 U.S.C. § 77h). If the SEC determines that an issuer has misstated or omitted in a registration statement any material fact that would be required to make

can subsequently offer its securities for sale, but must provide to all purchasers a prospectus that includes the registration statement's information.[40]

In addition to registration provisions, the Securities Act also contains liability provisions.[41] Section 11 of the Securities Act makes unlawful any misstatement or omission of material fact in the registration statement.[42] Similarly, Section 12(a)(2) prohibits any misstatement or omission of material fact in communications relating to the distribution of securities in interstate commerce.[43] Notably, these provisions create a dual-enforcement structure allowing for both public enforcement by the SEC as well as private lawsuits brought by individual investors.[44]

2. The Securities Exchange Act of 1934

In contrast to the Securities Act's focus on the initial public offering of securities, the Exchange Act focuses on disclosures that occur after an issuer's introduction of securities to the market.[45] The Exchange Act requires issuers of

---

the registration statement not misleading, the SEC is empowered to issue a stop order. Jones v. SEC, 298 U.S. 1, 15 (1936). The stop order defers the effectiveness of the registration statement until that registration statement is amended to comply with the requirements of the stop order. Securities Act of 1933 § 8(d), 15 U.S.C. § 77h(d); *Jones*, 298 U.S. at 15.

[40] Anderson, *supra* note 28, at 322. Section 10 of the Securities Act specifies in relevant part that a prospectus must include the information put forth in the registration statement. Securities Act of 1933 § 10, 15 U.S.C. § 77j. Aside from explicit exceptions listed in Section 3 of the Securities Act, this requirement is unconditional. Gustafson v. Alloyd Co., 513 U.S. 561, 569 (1995); *see supra* note 36 and accompanying text (discussing exemptions). Furthermore, the United States Supreme Court has provided that a "prospectus" includes those documents that speak to public offerings by the registrant or its majority stockholders. *Gustafson*, 513 U.S. at 569. The registration statement and the prospectus must outline the issuer's operations, the type of securities held out for sale, and disclose the firm handling the offering (and its financial stake in the offering). Anderson, *supra* note 28, at 323. Although the statute articulated certain information the registration statement and prospectus must include, it empowered the SEC with authority to revise the requirements. *Id.* at 322 (citing Securities Act of 1933 §§ 7, 10, sched. A, 15 U.S.C. §§ 77g, 77j, 77aa).

[41] Securities Act of 1933 §§ 11, 12(a)(2), 15 U.S.C. §§ 77k(a), 77l(a)(2); *see* Turk & Woody, *supra* note 32, at 969–70 (noting that the Securities Act is bifurcated into registration and liability provisions).

[42] Securities Act of 1933 § 11, 15 U.S.C. § 77k(a). For a description of the materiality standard, see *supra* note 18 and accompanying text.

[43] Securities Act of 1933 § 12(a)(2), 15 U.S.C. § 77l(a)(2).

[44] *See* Turk & Woody, *supra* note 32, at 970 (discussing how the provisions of the Securities Act make available as remedies both privately-initiated lawsuits and SEC enforcement actions); *see also* Bateman Eichler, Hill Richards, Inc. v. Berner, 472 U.S. 299, 310 (1985) (quoting J.I. Case Co. v. Borak, 377 U.S. 426, 432 (1964)) (highlighting the importance of private actions as the "most effective weapon" in enforcing the federal securities laws). The Supreme Court has described private investor lawsuits as a required parallel to the SEC's enforcement authority. *Borak*, 377 U.S. at 432. The SEC's enforcement powers include issuing administrative cease-and-desist orders governed by Section 8A of the Securities Act, and civil prosecutions in federal court governed by Section 20 of the Securities Act. COX ET AL., *supra* note 36, at 7.

[45] Turk & Woody, *supra* note 32, at 970 (contrasting the Securities Act's focus on disclosures during the IPO with the Exchange Act's focus on disclosures after the IPO). The Great Depression's

outstanding securities to register them and file periodic reports with the SEC.[46] The purpose of periodic reporting is to update the information that was offered in the issuer's registration statement.[47] Issuers are required to file their periodic reports only with the SEC, and are not required to send them directly to investors.[48] Nonetheless, advocates of the Exchange Act believed that individual investors would—and still do—benefit under this scheme.[49] In its original

serious consequences for the market did not result solely from new security offerings; then-outstanding securities greatly declined in value. *See* COX ET AL., *supra* note 36, at 7 (describing the decline in value experienced by securities listed on the New York Stock Exchange from eighty-nine billion dollars prior to the 1929 stock market crash to fifteen billion dollars thereafter). There is, however, an important distinction between the Securities Act and the Exchange Act. *Id.* at 9. The Securities Act delegates to the Federal Trade Commission the specific critical task of registering IPOs subject to the Securities Act's provisions; the goal, and how it is to be achieved, are clearly defined in the Securities Act. *Id.* In contrast, some view the Exchange Act as "a laundry list of problems" that Congress created the SEC to address. *Id.*

[46] Anderson, *supra* note 28, at 327. Under current law, the three classes of companies that are subject to the Exchange Act's requirements are companies having: (1) a class of securities registered on a national securities exchange; (2) assets exceeding ten million dollars and having "a class of equity securities held by at least 2000 record holders"; and (3) filed a registration statement under the Securities Act "that has become effective." COX ET AL., *supra* note 36, at 10. If a company meets any of the three criteria, it is referred to as a "reporting company" due to its regular reporting obligations under the Exchange Act, and must register with the SEC. *Id.*

[47] Anderson, *supra* note 28, at 327. Three of the most significant mandatory periodic filings are the Annual Report on Form 10-K, the Quarterly Report on Form 10-Q, and the Current Report on Form 8-K. COX ET AL., *supra* note 36, at 11; *see supra* note 33 and accompanying text (identifying the three most common mandatory periodic reports). The Form 10-K offers a "comprehensive overview of the company's business and financial condition and includes audited financial statements." *Fast Answers: Form 10-K*, U.S. SEC. & EXCHANGE COMMISSION, https://www.sec.gov/fast-answers/answers-form10khtm.html [https://perma.cc/H33N-FFJD]. The Quarterly Report on Form 10-Q, "filed for each of the first three fiscal quarters" of an issuer's financial year, offers a "continuing view" of the company's status throughout the fiscal year and includes unaudited financial information. *Fast Answers: Form 10-Q*, U.S. SEC. & EXCHANGE COMMISSION, https://www.sec.gov/fast-answers/answersform10qhtm.html [https://perma.cc/VDA4-LRYS]. Reporting companies must file a Current Report on Form 8-K to disclose the occurrence of certain material events that fall outside the reporting timeline of Forms 10-K and 10-Q. *Fast Answers: Form 8-K*, *supra* note 1. Moreover, the Exchange Act requires reporting companies to adhere to disclosure requirements regarding shareholder proxy solicitation. COX ET AL., *supra* note 36, at 11.

[48] COX ET AL., *supra* note 36, at 10 (noting that the Exchange Act contains no requirement that filings be submitted to investors or other market participants). Reporting companies are only required to file the required reports with the SEC. Anderson, *supra* note 28, at 328; *see* Mastronardi, *supra* note 10, at 340 (explaining that reporting companies are not required to submit filings directly to investors).

[49] *See* Anderson, *supra* note 28, at 328 (noting that, in the absence of a requirement that periodic reports be sent directly to investors, investors still ultimately receive the information contained in the reports because their investment advisors are financially incentivized to keep their clients informed). Furthermore, investors are thought to benefit from the mere availability of accurate information, regardless of whether individual investors actually review such information. *Id.* As most filings submitted to the SEC are publicly available through an SEC database, investors can access the filings, even if they are not sent directly to investors. *See About EDGAR*, U.S. SEC. & EXCHANGE COMMISSION, https://www.sec.gov/edgar/about [https://perma.cc/89UE-LTJU] (noting that the Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system indexes submissions of required filings by issu-

form, however, the Exchange Act applied only to the largest of companies—those entities listed on a national exchange.[50]

The Exchange Act also created the SEC, and vested it with vast authority to oversee the securities industry.[51] To facilitate the exercise of oversight, the Exchange Act authorized the SEC to promulgate regulations.[52] The SEC, organized into divisions and offices, carries out its mission through four primary divisions: Corporation Finance, Trading and Markets, Investment Management, and Enforcement.[53]

Like the Securities Act, the Exchange Act also contains liability provisions.[54] Section 10(b) contains the broad anti-fraud provision of the federal

---

ers to the SEC, but cautioning that not all filings submitted by public companies are available on EDGAR).

[50] *See* Anderson, *supra* note 28, at 343 (noting that the original version of the Exchange Act applied only to securities listed on an exchange, but not those publicly offered in OTC markets); Thompson & Sale, *supra* note 28, at 870–71 (explaining that the Exchange Act originally only applied to the most expansive companies). Consequently, the original version of the Securities Act did not capture all publicly-traded companies. *See* Thompson & Sale, *supra* note 28, at 870–71 (highlighting that the Securities Act encompassed all publicly held companies only after the enactment of the 1964 Amendments).

[51] Securities Exchange Act of 1934 § 4, 15 U.S.C. § 78d; *Fast Answers: The Laws That Govern the Securities Industry*, U.S. SEC. & EXCHANGE COMMISSION, https://www.sec.gov/answers/about-lawsshtml.html#secexact1934 [https://perma.cc/RHF9-23B4]. The SEC is an independent agency comprised of five commissioners. COX ET AL., *supra* note 36, at 14. The commissioners are appointed by the President of the United States to serve five-year terms, staggered such that one term expires every June and that no more than three commissioners are of the same political party as the president. *Id.*

[52] *See* Securities Exchange Act of 1934 § 10(b), 15 U.S.C. § 78j(b) (outlawing the use or employment, in connection with any security transaction, of "any manipulative or deceptive" device contrary to the rules and regulations the SEC puts forth as being in the public interest or achieving investor protection); Securities Exchange Act of 1934 § 13(b), 15 U.S.C. § 78m (empowering the SEC to promulgate rules and regulations "necessary or appropriate" to protect investors and ensure fairness in the markets); *see also* Anderson, *supra* note 28, at 327 (noting that the Exchange Act vested the SEC with the authority to issue regulations relating to shareholder proxy solicitation).

[53] COX ET AL., *supra* note 36, at 15. The SEC's mission is to protect the investing community, ensure fairness and efficiency throughout the securities markets, and enable capital formation. *What We Do*, *supra* note 28. The Division of Corporation Finance is responsible for carrying out the federal securities laws' disclosure regime by reviewing the numerous reports filed with the SEC by regulated entities. COX ET AL., *supra* note 36, at 15. The Division of Trading and Markets is responsible for overseeing secondary trading markets. *Id.* The Division of Investment Management carries out the Investment Company Act and the Investment Advisers Act. *Id.*; *see* 15 U.S.C. §§ 80a-1 to -64 (regulating the conduct of investment entities, such as mutual funds, and mandating disclosure to the public of investment-related information); 15 U.S.C. §§ 80b-1 to -21 (regulating the conduct of investment advisers, requiring registration with the SEC and adherence to investor protection regulations). Lastly, the Division of Enforcement—the most publicly visible of the divisions—investigates and brings action against entities for violations of the federal securities laws. COX ET AL., *supra* note 36, at 15; *Division of Enforcement: About the Division*, U.S. SEC. & EXCHANGE COMMISSION, https://www.sec.gov/page/enforcement-section-landing [https://perma.cc/79HV-4XNU]. *See generally What We Do*, *supra* note 28.

[54] Securities Exchange Act of 1934 § 10(b), 15 U.S.C. § 78j(b); Turk & Woody, *supra* note 32, at 970–71 (describing Section 10(b), the anti-fraud provision of the Exchange Act).

securities laws.[55] Rule 10b-5, promulgated thereunder, makes unlawful, in connection with a security transaction, any misstatement or omission of material fact required "to make the statements . . . not misleading" under the circumstances.[56] Similar to Sections 11 and 12(a) of the Securities Act, Section 10(b) and Rule 10b-5 are enforceable through both private causes of action and public enforcement action.[57] SEC-regulated entities can consequently be held liable for deficient disclosure both by private parties and the SEC.[58]

---

[55] Turk & Woody, *supra* note 32, at 970–71. Section 10(b) of the Exchange Act makes unlawful the use or employment of any manipulative or deceptive device, in connection with a security transaction, in violation of any SEC rule or regulation. Securities Exchange Act of 1934 § 10(b), 15 U.S.C. § 78j(b). This language in Section 10(b) empowered the SEC to promulgate Rule 10b-5. 17 C.F.R. § 240.10b-5; *see* Mastronardi, *supra* note 10, at 345 (noting that Section 10(b) vested authority in the SEC to outlaw various forms of deceptive conduct by enacting its own rules and regulations).

[56] 17 C.F.R. § 240.10b-5. The SEC adopted Rule 10b-5 in 1942. COX ET AL., *supra* note 36, at 695. Rule 10b-5 governs all forms of fraud relating to the transaction of securities. *Id.* at 695–96. Consequently, its reach is substantial. *See* Turk & Woody, *supra* note 32, at 971–72 (describing Rule 10b-5 as the "biggest stick" in federal securities regulation).

[57] *See* COX ET AL., *supra* note 36, at 696 (explaining that Rule 10b-5 is enforceable both by the SEC and through an "implied private right of action"); Turk & Woody, *supra* note 32, at 970 (noting that the liability provisions of the Securities Act can be enforced both by private lawsuits as well as SEC enforcement actions). There are, however, some differences between liability under the Securities Act and liability under the Exchange Act. *See* Turk & Woody, *supra* note 32, at 971–72 (identifying and discussing several differences between the liability provisions of the Securities Act and the liability provisions of the Exchange Act). For example, Section 10(b)'s verbiage does not allow for a private right of action by investors, although courts have long read an implied right of action into its language; Sections 11 and 12 of the Securities Act differ in this respect. *See id.* at 971 (citing *Blue Chip Stamps*, 421 U.S. at 723) (noting that the express language of Sections 11 and 12 of the Securities Act provide for private lawsuits by investors). To establish a violation of Section 10(b), a plaintiff must demonstrate: (1) a material misstatement or omission; (2) made with scienter; (3) in connection with the transaction of a security; (4) upon which the plaintiff relied; (5) to plaintiff's economic loss; and (6) which caused plaintiff's economic loss. Dura Pharm., Inc. v. Broudo, 544 U.S. 336, 341–42 (2005). Moreover, the United States Department of Justice can bring criminal sanctions in response to violations of Section 10(b). Turk & Woody, *supra* note 32, at 971–72; *see Blue Chip Stamps*, 421 U.S. at 737 (describing Rule 10b-5 as "a judicial oak which has grown from little more than a legislative acorn").

[58] Turk & Woody, *supra* note 32, at 971–72; *see Section 10(b) Litigation: The Current Landscape*, AM. B. ASS'N (Oct. 20, 2014), https://www.americanbar.org/groups/business_law/publications/blt/2014/10/03_kasner/ [https://perma.cc/YS79-QT2L] (noting that Section 10(b) lawsuits initiated by investors are a thorn in the side of publicly-traded entities). A typical lawsuit brought by a private investor involves an allegation of a misstatement or omission of material fact in a periodic report such as a Form 10-K or 10-Q. *See* Thompson & Sale, *supra* note 28, at 898–99 (stating that most of the securities fraud cases the authors studied raised allegations of material misstatement or omissions happening in the ordinary course of business).

3. Further Developments in Mandatory Disclosure

a. 1964: SEC Requirements Extended to Over-the-Counter Markets

The SEC has continued to emphasize disclosure.[59] In 1964, the Exchange Act was expanded to apply to over-the-counter markets, where securities not listed on an exchange are traded.[60] The newly enacted Section 12(g) of the Exchange Act effectuated this extension in coverage by requiring any class of securities to register with the SEC if it was held by at least 750 shareholders and issued by an entity having assets exceeding one million dollars.[61] Prior to this expansion, companies could avoid the SEC's jurisdiction by delisting their securities from the exchanges.[62] With the 1964 Amendments, however, the SEC could enforce more stringent requirements against a broader array of companies.[63]

---

[59] *See* Mastronardi, *supra* note 10, at 341–42 (describing further developments in the SEC's mandatory disclosure regime throughout the second half of the twentieth century).

[60] *See* Securities Acts Amendments of 1964, Pub. L. No. 88-467, 78 Stat. 565 (codified as amended at 15 U.S.C. §§ 77a-78lll) (stating that the purpose of the amendments was to extend the Acts' mandatory disclosure obligations to additional issuers). Before the 1964 Amendments, the Exchange Act governed only those entities with securities traded on a national exchange, and securities traded OTC were therefore not covered. Lee J. Sclar, *The Securities Acts Amendments of 1964: Selected Provisions and Legislative Deficiencies*, 53 CALIF. L. REV. 1494, 1496 (1965). A vast trading volume occurred in the OTC markets. *See* Allen Ferrell, *Mandatory Disclosure and Stock Returns: Evidence from the Over-the-Counter Market*, 36 J. LEGAL STUD. 213, 219 (2007) (noting that the OTC market generated $38.9 billion in sales in 1961). Given the significant trading volume and minimal information publicly available, the OTC market was ripe for exploitation. *See id.* at 219–20 (citing a widely-regarded 1963 SEC study that revealed that over ninety percent of fraud cases the SEC reported between January 1961 and July 1962 featured entities whose securities were traded on OTC markets, and which were therefore not bound by the federal securities laws' disclosure obligations). At the request of Congress, the SEC carried out a vast examination of the securities markets, particularly the OTC market. Sclar, *supra*, at 1496. The report noted that a majority of companies trading on the OTC market either did not make disclosures to investors or provided disclosure that was in some way deficient. Ferrell, *supra*, at 220. Therefore, among other recommendations, the report advocated for the application of the Exchange Act's periodic reporting obligations to OTC markets. *Id. See generally Company Directory*, OTC MARKETS, https://www.otcmarkets.com/corporate-services/company-directory [https://perma.cc/N7P8-T978] (listing companies traded in an OTC market).

[61] Securities Acts Amendments of 1964, § 3(c); Sclar, *supra* note 60, at 1497. On July 1, 1966, these registration requirements were also extended to apply to any class with at least five hundred shareholders. Sclar, *supra* note 60, at 1497. Altogether, the 1964 Securities Amendment extended disclosure obligations to all public companies. Thompson & Sale, *supra* note 28, at 871 & n.47. The SEC subsequently increased the assets minimum to ten million dollars. *See* 17 C.F.R. § 240.12g-1 (instructing that an issuer need not register with the SEC if its total assets are not more than ten million dollars).

[62] *See* Anderson, *supra* note 28, at 343 (noting that, prior to the 1964 Securities Amendments, many companies would simply delist their securities rather than submit to the SEC's "stringent disclosure standards").

[63] *See* Sclar, *supra* note 60, at 1497 (providing that the 1964 Amendments enabled the application of the Exchange Act's requirements to both listed and OTC securities). The SEC also shifted its emphasis towards mandatory disclosure as a means of enabling investment analysis by members of the investing public. *See* Mastronardi, *supra* note 10, at 341 (explaining that SEC regulation began to

b. 1982: Integration at Last

Decades after the enactments of the Acts, opponents of the disclosure regime criticized the redundancy of their requirements.[64] Until the 1980s, the requirements of the Acts were enforced separately, and issuers, therefore, incurred duplicative reporting obligations.[65] Consequently, in the 1970s, the SEC began to contemplate an integrated disclosure regime that would cut down on the repetitive requirements.[66]

In 1982, the SEC enacted Regulation S-K, a scheme of integrated disclosure.[67] Upon its release, the SEC indicated that Regulation S-K's objective was to lessen the burden on issuers by reducing duplicative disclosure require-

---

emphasize the role of mandatory disclosure in assessing investment decisions). As part of this change in tone, the SEC dialed back some of its requirements that mandatory disclosures need to be framed negatively and related only to "hard facts." Anderson, *supra* note 28, at 343; *see* Mastronardi, *supra* note 10, at 341 n.48 (explaining that "hard facts" are the opposite of "soft information," which is information that cannot be assessed objectively). The securities markets became increasingly sophisticated, resulting in an increased demand for advanced forms of modeling and analysis. Anderson, *supra* note 28, at 343. Despite this increasing sophistication, concerns for investor protection remained. *See id.* (noting that the SEC acknowledged that disclosure is still an effective form of investor protection). In so doing, the SEC recognized the informal value of disclosure and the fact that directly regulating conduct is the most effective way to prevent fraudulent and abusive behaviors. *See id.* at 343 & n.158 (noting that the SEC began to directly regulate abusive selling practices).

[64] *See* Milton H. Cohen, *"Truth in Securities" Revisited*, 79 HARV. L. REV. 1340, 1341–42 (1966) (arguing that the disclosure obligations created by the Acts are duplicative, and that an integrated statutory scheme is more efficient). *"Truth in Securities" Revisited* was highly influential, and the SEC echoed its call for an integrated disclosure system in its 1969 Disclosure Policy Study, also known as the Wheat Report. *See* U.S. SEC. & EXCH. COMM'N, REPORT ON REVIEW OF DISCLOSURE REQUIREMENTS IN REGULATION S-K, at 9 (2013), https://www.sec.gov/files/reg-sk-disclosure-requirements-review.pdf [https://perma.cc/2B4U-VXX7] (discussing the Wheat Report, which called for the expansion of Form S-7—the SEC's "first streamlined registration form"—and greater consolidation of the Acts' requirements).

[65] *See* U.S. SEC. & EXCH. COMM'N, *supra* note 64, at 10 (noting that Regulation S-K represented the introduction of uniform requirements for registration statements and periodic reports). Not only was redundant information required, but the form in which it was to be presented varied between the Acts' two sets of requirements. John C. Coffee, Jr., *Re-Engineering Corporate Disclosure: The Coming Debate Over Company Registration*, 52 WASH. & LEE L. REV. 1143, 1158 (1995). Similarly, although the Acts used some of the same terms to carry out its requirements, the terms were not defined consistently. *Id.*

[66] U.S. SEC. & EXCH. COMM'N, *supra* note 64 (describing a report issued by the SEC in 1977 that called for a unified mandatory disclosure regime); *see* Coffee, *supra* note 65, at 1145 (asserting that under the Exchange Act's scheme of continuous disclosure, logic would dictate that an issuer only be required to disclose material information not previously shared).

[67] *See* 17 C.F.R. §§ 229.10–.1208 (encompassing the entirety of Regulation S-K); Thompson & Sale, *supra* note 28, at 873–74 (discussing the disclosure regime implemented by Regulation S-K). The SEC implemented the first version of Regulation S-K in 1977, although it was reshaped and extended in 1982. U.S. SEC. & EXCH. COMM'N, *supra* note 64, at 10. Similarly, the SEC implemented Regulation S-X, providing requirements for accounting standards, as part of the regime of integrated disclosure. Turk & Woody, *supra* note 32, at 972 n.69; *see* 17 C.F.R. §§ 210.1-01–.12.29 (encompassing the entirety of Regulation S-X).

ments.[68] To effectuate this goal, Regulation S-K established numerous substantive requirements covering the non-financial items that an issuer must disclose in corporate filings with the SEC.[69] Regulation S-K eliminated redundancies by creating one unified set of disclosure obligations for the initial registration under the Securities Act and the further periodic reporting under the Exchange Act.[70]

Under Regulation S-K, issuers are obligated to disclose to the SEC—and by extension to investors—a large volume of information covering numerous subjects, such as pending legal proceedings and corporate governance information.[71] Although Regulation S-K covers a broad array of subject matter, disclosure is limited to material information—information that a reasonable investor is substantially likely to consider important in determining whether to purchase or sell the registered security.[72] Failure to adhere to these requirements by omitting or misstating any material information could result in liability under federal securities law.[73]

---

[68] *See* Adoption of Integrated Disclosure System, Securities Act Release No. 33-6383, 47 Fed. Reg. 11,380, 11,382 (Mar. 3, 1982) (stating that the goal of Regulation S-K was to alleviate registrants' burdens under the Acts by removing duplicative reporting obligations while also ensuring that investors receive "meaningful nonduplicative information" to make investment determinations).

[69] *See* U.S. SEC. & EXCH. COMM'N, *supra* note 64, at 8 (noting that Regulation S-K governs non-financial statement disclosure obligations); Thompson & Sale, *supra* note 28, at 873–74 (noting that, with the passage of Regulation S-K, the SEC regulates both the timing and content of disclosures); Turk & Woody, *supra* note 32, at 972 n.69 ("Reg[ulation] S-K demands a formidable amount of disclosure regarding corporate operations, governance structures, financial information, pending legal proceedings, corporate officers and board members, among numerous other topics.").

[70] Roberta S. Karmel, *Disclosure Reform—The SEC Is Riding Off in Two Directions at Once*, 71 BUS. LAW. 781, 785 (2016).

[71] *See* Turk & Woody, *supra* note 32, at 972 n.69 (citing 17 C.F.R. §§ 229.10–.1208; Amendments to Annual Report Form, Related Forms, Rules, Regulations, and Guides, SEC Release No. 33-6231, 45 Fed. Reg. 63630 (Sept. 25, 1980); Adoption of Integrated Disclosure System, Securities Act Release No. 33-6383, 47 Fed. Reg. 11380 (Mar. 3, 1982)) (highlighting the substantive requirements of Regulation S-K); Mastronardi, *supra* note 10, at 342 (stating that Regulation S-K includes numerous obligations for substantive disclosure); *supra* notes 48–49 and accompanying text (noting that reporting companies are not explicitly required to disclose information directly to investors).

[72] Karmel, *supra* note 70, at 785–86 (quoting 17 C.F.R. § 230.405). Registrants do not need to conduct an independent assessment of the materiality of any information that is required—a fixed line item—under Regulation S-K. *Id.* at 786. SEC Rule 12b-20, however, requires companies to disclose any further information that is needed to make the statements not misleading given the circumstances under which they are put forth. 17 C.F.R. § 240.12b-20; *see* Karmel, *supra* note 70, at 786 (explaining that reporting companies oftentimes need to go further than the line-item requirements of Regulation S-K).

[73] *See* Turk & Woody, *supra* note 32, at 974 (noting that the SEC can police violations of Regulation S-K); Mastronardi, *supra* note 10, at 342 (specifying that, although Regulation S-K compels disclosure of a wide range of information, it is limited to information that is material). To make out a claim of fraud under Section 10(b) of the Exchange Act, a plaintiff must demonstrate, among other elements, that the defendant made a misstatement or omission of *material* fact, and with scienter. Mastronardi, *supra* note 10, at 345 (emphasis added).

B. Why Disclosure?: Understanding the Rationale for Federal Securities Regulation

Federal securities regulation is premised upon a mandatory disclosure regime: the law creates a duty for issuers to disclose certain information at specific times.[74] A principal justification for this system is that the mandatory disclosure regime makes markets more efficient by decreasing the asymmetry of information between issuers and investors.[75] Mandatory disclosure equalizes investors' access to information, and makes that information easier to digest.[76] Another common argument is that mandatory disclosure protects investors from abusive practices, such as exploitation.[77]

Although mandatory disclosure remains foundational to the SEC's regulatory efforts, its efficacy is still debated.[78] One of the strongest arguments against mandatory disclosure centers on its role in dispersing information to investors.[79] Critics of the disclosure regime argue that information already flows to investors without any regulations to compel disclosure.[80] This counterargument asserts that a company is independently motivated to disclose material information to its investors, regardless of SEC requirements, because

---

[74] *See* Turk & Woody, *supra* note 32, at 968–69 (identifying the mandatory disclosure scheme as the primary mechanism for carrying out the goals of the federal securities laws). The system, however, is structured such that issuers are obligated to disclose only when affirmative law creates such an obligation. *See* Gallagher v. Abbott Labs., 269 F.3d 806, 808 (7th Cir. 2001) ("We do not have a system of continuous disclosure. Instead firms are entitled to keep silent (about good news as well as bad news) unless positive law creates a duty to disclose.").

[75] Turk & Woody, *supra* note 32, at 969 n.49 (citing Cynthia A. Williams, *The Securities and Exchange Commission and Corporate Social Transparency*, 112 HARV. L. REV. 1197, 1199–200 (1999)); Mastronardi, *supra* note 10, at 343 (noting that mandatory disclosure enables the proliferation of access to truthful information, thereby making markets more efficient). Moreover, at the same time, costlier and more stringent regulatory intervention is avoided. Turk & Woody, *supra* note 32, at 969 n.49. *See generally* Easterbrook & Fischel, *supra* note 10, at 692–96 (describing, and arguing against, some of the common justifications raised in support of the mandatory disclosure regime). Frank Easterbrook & Daniel Fischel ultimately find several of the common rationales to be unpersuasive, and put forward several alternative rationales in support of mandatory disclosure, including a cap on the costs generated by the common law regime and the prevention of interstate manipulation. *Id.*

[76] *See* Easterbrook & Fischel, *supra* note 10, at 694 (noting that disclosure requirements mandate simple presentation of and equal access to information, in theory enabling anyone to understand it and thus helping to prevent the manipulation of lay investors).

[77] *See* Cohen, *supra* note 64, at 1367–68 (noting that the regime of mandatory disclosure purports to protect investors in all facets of securities trading); Easterbrook & Fischel, *supra* note 10, at 693–95 (describing an argument that providing information to investors equips them to fend for themselves against abuse).

[78] Mastronardi, *supra* note 10, at 343–45. Moreover, even advocates disagree over the optimal level of disclosure. *See id.* (describing the disagreement over the most effective level of disclosure needed to generate the most efficiency in the securities markets).

[79] *See id.* at 344 (describing a common counterargument to mandatory disclosure: that it is not needed to stimulate information's dissemination).

[80] *Id.*

doing so will generate higher profits.[81] Another criticism of disclosure obligations is that they are detrimental to the market because the volume of information required by them overwhelms investors, rendering them unable to discern the information most important to their positions.[82] Critics also challenge mandatory disclosure's role in protecting investors from exploitation, claiming that unsophisticated investors, in fact, already enjoy the benefits of sophisticated investors' digestion of information released to the market, in the form of prices that incorporate all information obtainable about the underlying securities.[83]

C. Shifting Focus: The SEC Hones In on Cybersecurity

1. 2011 Cybersecurity Disclosure Guidance

On May 11, 2011, Senator John D. Rockefeller IV, Chairman of the Senate Committee on Commerce, Science, and Transportation ("Commerce Committee") urged the SEC to issue guidance pertaining to the disclosure of cybersecurity incidents.[84] A cybersecurity "incident" is defined as an incident that does have or potentially can have a negative impact on an entity's information system, or the data contained in that system.[85] The Commerce Committee's request noted that many issuers do not disclose cybersecurity-related incidents to their investors and cited a 2009 study that found that thirty-eight percent of Fortune 500 companies made a "significant oversight" in failing to address cybersecurity concerns in their filings with the SEC.[86] Therefore, the

---

[81] *Id.*

[82] *See id.* (describing the concern that a large volume of disclosure obligations will be detrimental to the securities market). In mandating disclosure of vast amounts of information, too many disclosure obligations could inundate investors with such a volume of information that investors will not be able to determine the relevancy of individual pieces of information. *Id.*

[83] Easterbrook & Fischel, *supra* note 10, at 694 ("The uninformed traders can take a free ride on the information impounded by the market: they get the same price received by the professional traders without having to do any of the work of learning information.").

[84] Letter from John D. Rockefeller IV et al., Senate Comm. on Commerce, Sci., & Transp., to Mary Schapiro, Chairman, U.S. Sec. & Exch. Comm'n 1 (May 11, 2011), https://www.commerce.senate.gov/public/_cache/files/4ceb6c11-b613-4e21-92c7-a8e1dd5a707e/41A8309A6FC78E9630AEEA660D81D379.5.11.11-letter-to-sec.pdf [https://perma.cc/8KEE-9S3D] (requesting that the SEC develop guidance pertaining to cybersecurity disclosure, particularly on the materiality of system and network hacks). The letter emphasized that cybersecurity was one of the period's most pressing issues. *See id.* (explaining that unauthorized parties attempt to misappropriate data to the detriment of businesses, individuals, and the economy as a whole). Due to the importance of the threat, the Committee requested clarification on the disclosure obligations for corporate issuers. *Id.*

[85] *Glossary*, NAT'L INITIATIVE FOR CYBERSECURITY CAREERS & STUD., https://niccs.us-cert.gov/about-niccs/glossary#I [https://perma.cc/7J2C-7D5B] (defining a cybersecurity "incident").

[86] Letter from John D. Rockefeller IV et al. to Mary Schapiro, *supra* note 84, at 1–2. The letter mentioned some filings that identified cybersecurity breaches, but stated that it noticed no filings that articulated steps to mitigate exposure to cybersecurity breaches. *Id.* at 2. Given the inconsistencies in reporting, the Committee asked that the SEC issue guidance clarifying disclosure requirements relating to cybersecurity concerns. *Id.*

Commerce Committee asserted, clarifying the obligations of SEC filers with respect to cybersecurity, that disclosure was paramount.[87] Shortly thereafter, on October 13, 2011, the Division of Corporation Finance issued guidance articulating its position on disclosure obligations regarding cybersecurity breaches.[88] Although it was issued by the SEC's staff, the 2011 guidance did not have the force or effect of law.[89]

The 2011 guidance first explained that the SEC's mandatory disclosure regime ensures timely disclosure of material cybersecurity information—that which a reasonable investor would view as significant in rendering a decision related to her investments.[90] Although no disclosure requirement then in existence explicitly governed cybersecurity issues, the 2011 guidance asserted that several disclosure requirements may nonetheless compel issuers to disclose such issues.[91] The 2011 guidance identified areas in which cybersecurity disclosure

---

[87] *See id.* (asserting that public company disclosure of material cybersecurity incidents is "inconsistent and unreliable" and requesting clarification from the SEC).

[88] Div. of Corp. Fin., *supra* note 12. The disclosure guidance was not, however, the first time the SEC acted with an eye towards cybersecurity. *See* Pierotti, *supra* note 3, at 410 (discussing the SEC's "safeguards rule," which it enacted in 2000). On November 13, 2000, the SEC enacted the "safeguards rule," which created standards for financial institutions' protection of consumer data. *Id.* The SEC updated the rule in 2005 to require institutions to develop and carry out "'written policies and procedures'" covering the safeguards the institutions will take to protect consumer information. *Id.* (quoting 17 C.F.R. § 248.30(a)). The policies must be reasonably calculated to: (1) afford security and confidentiality for the data; (2) protect against potential cybersecurity threats; and (3) stop any unapproved "access to or use of the data that could cause substantial harm or inconvenience." *Id.* In the decades following its promulgation of the safeguards rule, however, the SEC brought few actions under its auspices. *Id.* (noting that the SEC brought only three enforcement actions under the safeguards rule in the ten years after it came into effect).

[89] *See* Div. of Corp. Fin., *supra* note 12 (stating that the guidance reflects only the perspective of the SEC's Division of Corporation and not that of the SEC at large). Moreover, the guidance explicitly stated that the SEC took no position on its substance. *See id.* (asserting that the SEC has "neither approved nor disapproved" of the information put forth in the 2011 Division of Corporation Finance guidance).

[90] *See id.* (noting that one of the purposes of the Acts is to ensure full and complete disclosure of material information about risks and events). Assessing the materiality of cybersecurity incidents requires consideration of factors such as the incident's scale, the information subject to the breach, and the possible effect on the reporting company's operations. Daniel F. Schubert, Jonathan G. Cedarbaum & Leah Schloss, *The SEC's Two Primary Theories in Cybersecurity Enforcement Actions*, CYBERSECURITY L. REP., Apr. 8, 2015, at 1, 3, https://www.wilmerhale.com/en/insights/publications/the-secs-two-primary-theories-in-cybersecurity-enforcement-actions [https://perma.cc/5QEM-4QWJ].

[91] Div. of Corp. Fin., *supra* note 12 ("Although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents."); SULLIVAN & CROMWELL LLP, SEC ISSUES EXPANDED INTERPRETIVE GUIDANCE ON CYBERSECURITY MATTERS 1–2 (Feb. 27, 2018), https://www.sullcrom.com/siteFiles/Publications/SC_Publication_SEC_Issues_Expanded_Interpretive_Guidance_on_Cybersecurity_Matters.pdf [https://perma.cc/JQK6-DEJC] (noting that cybersecurity issues are implicated by the federal securities laws, despite the fact that the latter technically do not speak of the former). Issuers are required to disclose material information relating to cybersecurity incidents that are necessary to make other disclosed statements not misleading in light

would be warranted: those involving risk factors, management's discussion and analysis of financial condition and results of operations ("MD&A"), description of business, legal proceedings, financial statement disclosure, and disclosure control and procedures.[92]

Under Item 503(c) of Regulation S-K, an SEC registrant must discuss in filings with the SEC the attributes rendering an investment in the company "speculative or risky."[93] In the risk factor section, the Commission stated that if cybersecurity risks are some of the most significant hazards that make an investment with an issuer "speculative or risky," that issuer should disclose the risk of cybersecurity incidents.[94] In so doing, the issuer should consider past cybersecurity breaches, their severity, and the likelihood of future breaches.[95] In the MD&A section, the Commission stated that an issuer should disclose cybersecurity risks to the extent they reflect a "material event, trend, or uncertainty that is reasonably likely to have a material effect" on the registrant's financial outlook.[96] In the description of business section, the SEC instructed issuers to note if a cybersecurity incident would have a material effect on aspects of an issuer's business.[97] In the legal proceeding section, the SEC advised that an issuer should disclose any material pending litigation in which the registrant or its subsidiaries is a party and which stems from a cybersecurity incident.[98] In the financial statement disclosure section, the SEC instructed issuers to consider carefully when disclosure of a cybersecurity incident is required, given the potential effect such an incident could have on a corporation's balance sheet.[99] Lastly, in the disclosure controls and procedures section, the guidance instructed issuers to disclose information relating to the effective-

---

of their circumstances. Div. of Corp. Fin., *supra* note 12. Furthermore, generic language is inappropriate: issuers must describe their cybersecurity issues in terms specifically applicable to the issuers. *Id.*

[92] Div. of Corp. Fin., *supra* note 12 (providing guidance for cybersecurity-related disclosures that are captured by other disclosure obligations mandated by the federal securities laws); *see* 17 C.F.R. §§ 229.10–.1208 (setting forth the entirety of Regulation S-K's requirements). *See generally* Benjamin A. Powell et al., *SEC Issues New Guidance on Disclosing Cybersecurity Risks and Incidents*, WILMERHALE (Oct. 27, 2011), https://www.wilmerhale.com/en/insights/publications/sec-issues-new-guidance-on-disclosing-cybersecurity-risks-and-incidents-october-27-2011 [https://perma.cc/DKE6-ZZB6] (summarizing the 2011 SEC Cybersecurity guidance).

[93] 17 C.F.R. § 229.503.

[94] Div. of Corp. Fin., *supra* note 12.

[95] *Id.*

[96] *Id.*

[97] *See id.* (providing that an issuer should disclose to investors whether cybersecurity incidents, if experienced, have a material impact on the issuer's business).

[98] *See id.* (offering as an example of this requirement that the breach of voluminous consumer information, ultimately leading to "material litigation," would trigger disclosure obligations, including where the lawsuit was brought, when the litigation commenced, the parties to the lawsuit, the underling factual allegations, and the relief requested).

[99] *See id.* (noting that companies must consider whether disclosure is necessary when a cybersecurity incident is uncovered after financial statements are prepared, but before they are released).

ness of such controls and procedures, particularly to the extent cybersecurity incidents impact the issuer's ability to collect and report information to the SEC in mandatory periodic reports.[100]

The 2011 guidance established that cybersecurity risks impact nearly every aspect of an issuer's business.[101] Moreover, it confirmed that cybersecurity concerns affect not only companies, but also investors and the economy at large.[102] Senator Rockefeller, the author of the Senate Committee's letter to the SEC, responded positively to the guidance.[103] He believed that the 2011 guidance would profoundly alter the way companies address cybersecurity issues.[104] Indeed, following the issuance of the 2011 guidance, many corporate issuers started to include disclosures relating to cybersecurity incidents in their mandatory corporate filings.[105]

2. 2014–2016: Uptick in SEC Cybersecurity Activity

In 2014, the SEC affirmed the 2011 cybersecurity guidance at a roundtable on cybersecurity.[106] Then-Chairwoman of the SEC Mary Jo White stated that the Commission's jurisdiction over cybersecurity concerns extended to ensuring market integrity, protection of consumer data, and disclosure of material information.[107] White also affirmed the SEC's ongoing commitment to further

---

[100] *Id.* By way of example, the Division of Corporation Finance noted that "if it is reasonably possible that information would not be recorded properly due to a cyber incident affecting a registrant's information systems, a registrant may conclude that its disclosure controls and procedures are ineffective." *Id.*

[101] *See id.* (describing the disclosure requirements of periodic reports implicated by cybersecurity incidents, despite the fact that the requirements themselves do not specifically address cybersecurity).

[102] *See* Powell et al., *supra* note 92 (noting that the 2011 guidance emphasizes cybersecurity's implications for the economy at large, not only for companies).

[103] *See* Press Release, U.S. Senate Comm. on Commerce, Sci., & Transp., Rockefeller Says SEC Guidance Fundamentally Changes the Future of Cybersecurity (Oct. 13, 2011), https://www.commerce.senate.gov/public/index.cfm/2011/10/rockefeller-says-sec-guidance-fundamentally-changes-the-future-of-cybersecurity [https://perma.cc/ATU3-N5EX] (stating that Senator Rockefeller was "pleased" that the SEC acted on the Senate Committee's request).

[104] *See id.* (stating that the 2011 Division of Corporation Finance guidance "changes everything" because it will enable market assessment of public companies based on, among other criteria, companies' cybersecurity prowess).

[105] Commission Statement and Guidance on Public Company Cybersecurity Disclosure, 83 Fed. Reg. at 8167 (noting that many companies addressed cybersecurity issues in their disclosures, mostly in the risk factors section, after the 2011 guidance); SULLIVAN & CROMWELL LLP, *supra* note 91, at 2 (stating that after the 2011 release many issuers began to disclose cybersecurity breaches, generally in the forward-looking statement or risk factors sections).

[106] *See* Mary Jo White, Chairman, U.S. Sec. & Exch. Comm'n, Remarks at U.S. Securities and Exchange Commission Cybersecurity Roundtable 9 (Mar. 26, 2014), https://www.sec.gov/spotlight/cybersecurity-roundtable/cybersecurity-roundtable-transcript.txt [https://perma.cc/6PU2-L97Z] (noting that the 2011 SEC guidance on cybersecurity compels disclosure of cybersecurity incidents that have a material impact on an issuer's operations and overall performance).

[107] *Id.*

development of its standards relating to cybersecurity concerns.[108] Following the roundtable, the SEC continued to focus on cybersecurity, issuing new guidance on the subject and even, in some instances, authoring comment letters that directed companies to disclose specific cybersecurity incidents.[109] For example, in 2012 the SEC issued a Comment Letter to Amazon.com, Inc. ("Amazon"), directing Amazon to disclose details of a cybersecurity attack faced by one of its subsidiaries, Zappos.com.[110] In response, Amazon provided revised disclosure about the Zappos.com incident.[111]

During the same period, the SEC also addressed cybersecurity through means other than disclosure.[112] In 2015, the SEC brought its first cybersecurity-related enforcement action against R.T. Jones Capital Equities Management, Inc. under Regulation S-P.[113] Promulgated by the SEC in 2000, Regulation S-P compels financial institutions to abide by policies that are "reasonably designed" to protect the sensitive personal information of consumers, to secure

---

[108] *See id.* (stating that, following the Division of Corporation Finance's 2011 guidance, the SEC continued to assess the importance of cybersecurity issues to SEC issuers, the securities markets, and investors, particularly with respect to cybersecurity-focused disclosure).

[109] *See* U.S. SEC. & EXCH. COMM'N, INVESTMENT MANAGEMENT GUIDANCE UPDATE 1–2 (2015), https://www.sec.gov/investment/im-guidance-2015-02.pdf [https://perma.cc/7BED-Z3GM] (addressing cybersecurity regulatory updates relevant to registered investment companies and advisers); Megan Gordon et al., *The Equifax Hack, SEC Data Breach, and Issuer Disclosure Obligations*, HARV. L. SCH. F. ON CORP. GOVERNANCE & FIN. REG. (Oct. 5, 2017), https://corpgov.law.harvard.edu/2017/10/05/the-equifax-hack-sec-data-breach-and-issuer-disclosure-obligations/#12 [https://perma.cc/L9XC-M27U] (pointing to a 2012 SEC comment letter compelling Amazon.com, Inc. to disclose cybersecurity incidents affecting its subsidiaries). The SEC utilizes two kinds of comment letters. *Fast Answers: Comment Letters*, U.S. SEC. & EXCHANGE COMMISSION, https://www.sec.gov/fast-answers/answerscommentlettershtm.html [https://perma.cc/8P5E-NC3J]. The first are those submitted to the SEC by people and companies in response to SEC requests for public comments as part of its rulemaking process. *Id.*; *see supra* note 16 (explaining these notice and comment rulemaking procedures). The second type of SEC comment letters include correspondence between the SEC and its regulated entities, made publicly available on EDGAR. *Fast Answers: Comment Letters*, *supra*. These comment letters can feature, for example, a request by the SEC for the regulated entity to disclose further information to help the SEC's review of the entity's corporate filings or an instruction to provide more disclosure in a future filing with the SEC. *Id.* These comment letters apply only to the specific filings in question. *Id.* Moreover, although the comment letters disclose the decisions of the SEC's staff, they are not official statements of the SEC's viewpoint. *Id.*

[110] *See* Amazon.com, Inc., SEC Comment Letter (Mar. 12, 2012) (obligating Amazon to fix items of disclosure in its Form 10-K for the fiscal year ended December 31, 2011).

[111] *See* Amazon.com, Inc., SEC Correspondence (May 3, 2012) (discussing future disclosure of cybersecurity incidents, particularly as a risk factor that Amazon faces); *see also* Amazon.com, Inc., SEC Correspondence (Apr. 9, 2012) (providing details about the Zappos.com cyber incident).

[112] *See* Gordon et al., *supra* note 109 (describing SEC enforcement actions and annual inspections that addressed cybersecurity concerns).

[113] *Id.*; *see* 17 C.F.R. § 248.30 (containing the SEC's requirements for safeguarding the sensitive personal information of consumers). The SEC enforcement action concerned the July 2013 breach of a third-party server R.T. Jones utilized to store sensitive, personal information of over one hundred thousand clients, which was made vulnerable to misappropriation. Gordon et al., *supra* note 109.

this information against anticipated breaches, and to prevent unapproved use of the information that could cause the consumer significant harm.[114]

Likewise, in 2016 the SEC brought action against Morgan Stanley, a registered investment adviser, for allegedly failing to safeguard appropriately the personal information of its consumers.[115] At the same time, the SEC emphasized cybersecurity issues in the annual inspections of registered investment advisers conducted by its Office of Compliance Inspections and Examinations.[116]

3. 2017–2018: Creation of the Cyber Unit and Issuance of the 2018 Cybersecurity Disclosures Guidance

In September 2017, SEC Chairman Jay Clayton released a report outlining a broad strategy for overseeing the cybersecurity policies of SEC-regulated entities.[117] The SEC report addressed five overarching points: (1) the type of information the SEC amasses and makes available to the public; (2) how the SEC balances and responds to its own cybersecurity risks; (3) how it considers cybersecurity in its supervision of regulated entities; (4) how it works with other regulators to diminish cybersecurity threats; and (5) how it wields its enforcement authority to protect investors and markets from abusive cybersecurity actors.[118] In the same document, Clayton reported that not even the SEC is

---

[114] 17 C.F.R. § 248.30; Gordon et al., *supra* note 109.

[115] Gordon et al., *supra* note 109. A former employee of Morgan Stanley downloaded personal information relating to over seven hundred thousand accounts to his personal server. Press Release, U.S. Sec. & Exch. Comm'n., SEC: Morgan Stanley Failed to Safeguard Customer Data (June 8, 2016), https://www.sec.gov/news/pressrelease/2016-112.html [https://perma.cc/UGA4-6NPH]. The former employee's personal server was ultimately hacked. *Id.* Following the hack, some of the stolen customer information was placed on the internet, accompanied by an offer to procure more stolen data for interested buyers. Pierotti, *supra* note 3, at 413. Although Morgan Stanley utilized written policies and procedures, it nonetheless violated the safeguards rules because those policies and procedures were not reasonably designed to protect the underlying consumer information. *See id.* at 413–14 (noting that Morgan Stanley's policies neither properly limited employee access nor logged how employees were utilizing the consumer information or when they accessed Morgan Stanley's systems).

[116] Gordon et al., *supra* note 109. The SEC began to zero in on cybersecurity issues during examinations in January 2014, when it requested that the firms it examined provide information relating to cybersecurity incidents, including, for example, any known cybersecurity risks, the firm's cybersecurity protections, any identified unauthorized access to the firm's network, and whether and how a firm reacted to a cybersecurity incident. *Id.* The following year, during the 2015 examination cycle, the SEC built on the 2014 approach, but it also assessed the procedures and controls utilized by firms to assess preparedness for cybersecurity incidents. *Id.*

[117] Clayton, *supra* note 11 (detailing the SEC's approach to five aspects of cybersecurity regulation).

[118] *See id.* (stating that the report would address cybersecurity risks and events faced by both SEC-regulated entities and the SEC itself). Like previous SEC statements, Chairman Clayton's cybersecurity statement reinforced the SEC's commitment to adequate disclosure by public companies of cybersecurity-related issues. *See id.* (stating that the SEC continues to assess the viability of the 2011 Division of Corporation Finance guidance while considering evolving cybersecurity concerns facing both issuers and the securities markets).

immune from cybersecurity incidents, acknowledging a 2016 breach of an SEC database.[119] Several days after the report, the Commission announced the creation of a new Cyber Unit within the Division of Enforcement.[120] This new unit was established to address cybersecurity-related misconduct, and was created in response to the Division of Enforcement's belief that cybersecurity concerns are one of the greatest modern threats to markets and their participants.[121]

Following the creation of the Cyber Unit, the SEC continued its focus on cybersecurity-related disclosure.[122] In February 2018, the SEC released new interpretive guidance pertaining to disclosures of cybersecurity risks and incidents.[123] This 2018 guidance affirmed the positions articulated by the SEC's

---

[119] *See id.* (addressing the cybersecurity breach the SEC experienced in 2016); *see also* Press Release, U.S. Sec. & Exch. Comm'n, SEC Brings Charges in EDGAR Hacking Case (Jan. 15, 2019), https://www.sec.gov/news/press-release/2019-1 [https://perma.cc/V8MH-4UZW] (describing a breach of an SEC database, thereby giving the hackers access to sensitive—and nonpublic—information). In 2016, unauthorized users gained access to EDGAR, the electronic storehouse for public filings submitted to the SEC. Press Release, *supra*. In its breach of EDGAR, the hackers gained access to confidential "test filings," which SEC registrants can submit to the SEC in advance of an actual filing to ensure EDGAR will correctly process the filings. *Id.* In gaining access to nonpublic financial information, the hackers earned over four million dollars in unlawful profits. *Id.* Although the SEC learned of the breach in 2016, it did not ascertain that the hackers could have utilized the information to make illicit trades until the following year. Renae Merle, *SEC Reveals It Was Hacked, Information May Have Been Used for Illegal Stock Trades*, WASH. POST (Sept. 20, 2017), http://wapo.st/2yt1mtEtid=ss_mail&utm_term=.82b4f3ce9952 [https://perma.cc/Y9Q5-QPFR]. Moreover, this incident was not the first breach of EDGAR. *Id.* (describing cybersecurity incidents in 2014 and 2015).

[120] Press Release, U.S. Sec. & Exch. Comm'n, SEC Announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors (Sept. 25, 2017), https://www.sec.gov/news/press-release/2017-176 [https://perma.cc/LLF3-4BA8]. On the same day, the SEC also announced the creation of a retail strategy task force, whose mission is to prevent abusive practices that target retail investors. *Id.*

[121] *See id.* (emphasizing the significant risk that cybersecurity poses to investors and the markets, and noting that the Cyber Unit will enhance the SEC's ability and expertise in the field). The Cyber Unit had a busy year in 2018, bringing twenty separate cybersecurity-related actions. *See* U.S. SEC. & EXCH. COMM'N, DIV. OF ENF'T, ANNUAL REPORT 7 (2018), https://www.sec.gov/files/enforcement-annual-report-2018.pdf [https://perma.cc/WD8C-STVB] (summarizing the Cyber Unit's efforts in fiscal year 2018).

[122] *See* Craig Newman, *SEC Cyber Briefing: Regulatory Expectations for 2019*, HARV. L. SCH. F. ON CORP. GOVERNANCE & FIN. REG. (Jan. 2, 2019), https://corpgov.law.harvard.edu/2019/01/02/sec-cyber-briefing-regulatory-expectations-for-2019/ [https://perma.cc/PBJ3-YDWC] (noting that the SEC released updated guidance for the disclosure of cybersecurity risks in February 2018).

[123] Commission Statement and Guidance on Public Company Cybersecurity Disclosure, 83 Fed. Reg. at 8166. The 2018 guidance was more authoritative than the 2011 guidance because it was authored by the SEC, whereas the Division of Corporation Finance prepared the 2011 guidance. EY CTR. FOR BD. MATTERS, ERNST & YOUNG LLP, SEC GUIDANCE ON CYBERSECURITY: BOARD CONSIDERATIONS 1 (2018), https://assets.ey.com/content/dam/ey-sites/ey-com/en_us/topics/cybersecurity/ey-sec-guidance-on-cybersecurity-board-considerations.pdf [https://perma.cc/GVZ5-VFEQ]. Moreover, the 2011 guidance did not reflect the official position of the SEC. *See* Div. of Corp. Fin., *supra* note 12 (stating that the guidance contained only the opinions of the Division of Corporation Finance and not that of the SEC).

Division of Corporation Finance in its 2011 guidance.[124] The 2018 guidance, however, added two new topics of interest: the significance of policies pertaining to cybersecurity, and prohibitions against insider trading in the context of cybersecurity.[125] The 2018 guidance cited these new areas of discussion as part of the underlying purpose of its issuance, in addition to reemphasizing the increasing relevance of its focus on cybersecurity.[126]

The SEC also reinforced the need for issuers to disclose cybersecurity risks that have a material significance to investors.[127] In assessing the materiality of cybersecurity incidents, the SEC stated that companies commonly balance factors such as the "nature, extent, and potential magnitude" of an identified cybersecurity incident—especially in light of the potential impact on corporate operations—as well as the kind of harm that could result from the incident.[128] Nevertheless, the SEC carefully noted that companies are not required to disclose sensitive information that could compromise their cybersecurity protection efforts.[129] The SEC, however, added a new, specific disclosure requirement that describes the role of the company's board of directors in overseeing and managing cybersecurity risk.[130]

In addition to disclosure requirements, the 2018 guidance emphasized the need for companies to have policies and procedures in place to determine the effect of any cybersecurity incidents on a company's operations and to assess

---

[124] *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosure, 83 Fed. Reg. at 8167 (noting that the 2018 guidance builds upon the Division of Corporation Finance's 2011 guidance). Reaffirming the 2011 guidance, the 2018 guidance stated that a company should be prepared to disclose cybersecurity risk in the following sections of certain periodic reports: "business and operations, risk factors, legal proceedings, management's discussion and analysis of financial condition and results of operations . . . financial statements, disclosure controls and procedures, and corporate governance." *Id.* at 8168.

[125] *Id.* at 8167.

[126] *See id.* at 8166–67 (noting that cybersecurity concerns affect investors, issuers, the securities markets, and the economy at large).

[127] *See id.* at 8168–69 (discussing how companies generally assess the materiality of cybersecurity incidents).

[128] *Id.* The SEC, however, did not provide how these factors are to be weighed, or whether others should be included. *See id.* (offering only minimal guidance on ascertaining an entity's cybersecurity-related disclosure obligations under the federal securities laws).

[129] *See id.* at 8169 (stating that the guidance does not require companies to disclose such detailed cybersecurity information to provide a "roadmap" that would help those attempting a cybersecurity attack).

[130] *Id.* at 8170 (affirming that a company must disclose the involvement of its board of directors in managing any material cybersecurity risks to which the company is exposed). Such an obligation arises from Item 407(h) of Regulation S–K and Item 7 of Schedule 14A, which mandate disclosure of the nature of a board of director's oversight of a company's risk. *Id.* Such oversight includes, for example, "how the board administers its oversight function and the effect this has on the board's leadership structure." *Id.*

the incidents' materiality to investors.[131] The SEC cited specific regulations that require companies to adopt such policies and procedures.[132] The guidance, however, did not identify specific cybersecurity controls and procedures that issuers should or could adopt to prevent cybersecurity incidents from occurring.[133]

The 2018 guidance also discussed the intersection of cybersecurity and insider trading.[134] It noted that information relating to cybersecurity may constitute material nonpublic information, and that companies should therefore carefully consider their insider trading policies to ensure no trading occurs based on this information.[135] In light of the sensitive implications of cybersecurity incidents for SEC registrants, the 2018 guidance cautioned against selective disclosure of material information concerning cybersecurity.[136]

---

[131] *Id.* at 8167. Such policies and procedures should act like an "'early warning system' to enable companies to determine" if a periodic report, such as a Current Report on Form 8-K, ought to be filed with the SEC. EY CTR. FOR BD. MATTERS, *supra* note 123.

[132] *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosure, 83 Fed. Reg. at 8171 (citing various regulations that define and require "disclosure controls and procedures"). For example, Exchange Act Rules 13a-15 and 15d-15 mandate that SEC-regulated companies adopt "disclosure controls and procedures" and, further, that managements routinely assess their efficacy. *Id.* (citing 17 C.F.R. §§ 240.13a-15, .15d-15). "Disclosure controls and procedures" are controls and procedures that seek to confirm that information an issuer is required to disclose in periodic reports under the Exchange Act is amassed and disclosed in a timely manner consistent with the SEC's rules and is similarly amassed and reported to an issuer's management in a timeframe that enables such timely disclosure (if management determines public disclosure is required). *Id.*

[133] *See id.* (describing company policies and procedures pertaining to cybersecurity, but not providing concrete examples of these policies and procedures).

[134] *See id.* at 8171–72 (discussing cybersecurity's implications for insider trading).

[135] *Id.* at 8171; *see* Newman, *supra* note 122 (summarizing the SEC's 2018 interpretive guidance). Insider trading is the unlawful practice whereby corporate insiders—such as officers, directors, or majority stockholders—trade securities based on material nonpublic information that would change the decision of the outsider had she been aware of said information. *See In re* Cady, Roberts & Co., 40 S.E.C. 907, 911 (1961) (providing that the insiders' failure to disclose material information to those with whom they deal creates liability under the federal securities laws). The insider either must disclose the material, nonpublic information or refrain from trading. *Id.*

[136] *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosure, 83 Fed. Reg. at 8172 (instructing SEC-regulated entities not to disclose selectively nonpublic information about cybersecurity incidents to individuals covered by Regulation FD—the SEC's fair disclosure regulation—prior to sharing that same information with the public). Regulation FD prohibits selective disclosure—disclosing material nonpublic information to certain enumerated individuals without also disclosing that information to the public at large. 17 C.F.R. § 243.100; *see* Commission Statement and Guidance on Public Company Cybersecurity Disclosure, 83 Fed. Reg. at 8172 (explaining Regulation FD). Regulation FD mandates that issuers that disclose material nonpublic information to certain individuals—brokers, dealers, investment advisers, investment companies, or stockholders when it is reasonably foreseeable the stockholders will make trading decisions based on the information—are required to disclose that same information to the public. Commission Statement and Guidance on Public Company Cybersecurity Disclosure, 83 Fed. Reg. at 8172 n.65 (citing 17 C.F.R. § 243.100). The SEC promulgated Regulation FD to address the possibility that companies would disclose material nonpublic information to specific individuals before making that same information available to the public. *Id.* at 8172. Such selective disclosure would allow those privy to the information either to profit from the information, or to avoid loss. Selective Disclosure and Insider Trading, Exchange Act Release No. 34-43154, 65 Fed. Reg. 51,716, 51,716 (Aug. 24, 2000). Regulation FD thereby seeks to

In April 2018, the SEC brought its first enforcement action for insufficient cybersecurity disclosure against the company formerly known as Yahoo!.[137] In December 2014, hackers breached the Yahoo! database and misappropriated the sensitive information of hundreds of millions of users.[138] Despite senior management learning of the breach within several days, Yahoo! did not disclose the existence of the breach to its investors through SEC filings until over two years later.[139] The SEC's complaint stated that Yahoo! was negligent in failing to make timely disclosure of the breach and for submitting misleading filings to the SEC.[140] Yahoo! ultimately settled with the SEC, agreeing to pay a thirty-five million dollar fine.[141]

---

prevent insider trading. *See id.* (noting that prior to Regulation FD, those who received advanced notice of certain sensitive corporate information—such as earnings results—either profited or escaped a loss to the detriment of those not privy to the same information).

[137] *See* Newman, *supra* note 122 (describing the SEC's enforcement action against Altaba Inc., formerly known as Yahoo!).

[138] Press Release, U.S. Sec. & Exch. Comm'n, Altaba, Formerly Known as Yahoo!, Charged with Failing to Disclose Massive Cybersecurity Breach; Agrees to Pay $35 Million (Apr. 24, 2018), https://www.sec.gov/news/press-release/2018-71[https://perma.cc/U2AJ-3JT5]; *see* Newman, *supra* note 122 (outlining the SEC's complaint and the underlying breach of the Yahoo! systems).

[139] Press Release, *supra* note 138; *see* Yahoo! Inc., Current Report (Form 8-K) (Sept. 22, 2016) (disclosing the breach to the SEC, and by extension to investors). On the same day Yahoo! disclosed the breach, its stock price fell three percentage points. Newman, *supra* note 122. It also caused Verizon Communications, Inc., which was in the process of acquiring the Yahoo!, to reduce its acquisition price by $350 million. *Id.*

[140] Newman, *supra* note 122. After learning of the breach, Yahoo! filed numerous periodic reports with the SEC, including quarterly and annual reports, in which the company failed to disclose the existence of the breach. Press Release, *supra* note 138. In lieu of disclosing the breach, Yahoo! asserted only that it faced the risk of cybersecurity breaches, as well as any associated adverse impact. *Id.* The SEC stated that Yahoo! informed neither its auditors nor outside counsel about the breach, actions it could have taken to ascertain the company's potential obligations to disclose under the federal securities laws. *Id.* Lastly, the SEC cited Yahoo!'s policies and procedures as inadequate to ensure that reports of cybersecurity incidents, or the risk of their potential occurrence, were considered in a timely fashion for possible disclosure in SEC filings. *Id.*

[141] Press Release, *supra* note 138. Yahoo!, however, neither admitted nor denied the charges in the SEC's complaint. *Id.* In addition to the SEC litigation, former officers and directors of Yahoo! also agreed to settle shareholder derivative lawsuits initiated in response to the breach. Craig A. Newman, *Lessons for Corporate Boardrooms from Yahoo's Cybersecurity Settlement*, N.Y. TIMES (Jan. 23, 2019), https://www.nytimes.com/2019/01/23/business/dealbook/yahoo-cyber-security-settlement.html [https://perma.cc/TT4P-DH6N]; *see* Kramer v. W. Pac. Indus., Inc., 546 A.2d 348, 351 (Del. 1988) (explaining that a derivative action is a suit brought by a shareholder on behalf of the corporation and thus any damages belong to the corporation). The lawsuits alleged that Yahoo!'s former officers and directors breached their fiduciary duties to the company by failing to make timely disclosure of the cybersecurity incidents, as well as by hiding the incidents from shareholders. Stipulation and Agreement of Settlement at 9, *In re* Yahoo! Inc. Shareholder Litig. (Cal. Super. Ct. Sept. 14, 2018) (17-CV-307054); Newman, *supra*. The settlement represented the first time shareholders successfully recovered monetary damages in derivative litigation resulting from a data breach. Newman, *supra*. In January 2019, a superior court judge in Santa Clara, California approved the settlement, pursuant to which former officers and directors of Yahoo! were ordered to pay twenty-nine million dollars, with eighteen million dollars ultimately going to Yahoo!'s successor-in interest, Altaba. *Id.* (noting that the settlement's remaining eleven million dollars will go to legal counsel). With respect to cybersecurity inci-

II. IMPLICATIONS OF THE SEC'S REGULATION OF CYBERSECURITY

Given the devastating consequences—financial and otherwise—of cybersecurity incidents, many industry leaders have stressed the importance of cybersecurity to American companies.[142] In recent years, the SEC has increased its attention to cybersecurity issues, a trend that is expected to continue.[143] This Part demonstrates that the SEC's 2018 guidance has implications extending be-

---

dents, claims not otherwise viable under federal law may be pursued through state law derivative actions. Edward A. Morse et al., *SEC Cybersecurity Guidelines: Insights into the Utility of Risk Factor Disclosures for Investors*, 73 BUS. LAW. 1, 18 (2018) (discussing the state law theory that can be utilized to pursue cases stemming from cybersecurity incidents). Like Yahoo!, Marriott also faces derivative liability in the wake of the recently disclosed breach of the Starwood guest reservation database. Jennifer Bennett, *Marriott Hit with Derivative Suit Over Massive Data Breach*, BLOOMBERG (Mar. 18, 2019), https://www.bloomberglaw.com/document/XF46GBAK000000?bna_news_filter=securities-law&jcsearch=BNA%25200000016991bad8f7ab7dd9ff047d0002#jcite [https://perma.cc/8YZ9-BJH2].

[142] *See* COUNCIL OF ECON. ADVISERS, EXEC. OFFICE OF THE PRESIDENT OF THE U.S., THE COST OF MALICIOUS CYBER ACTIVITY TO THE U.S. ECONOMY 1 (2018), https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf [https://perma.cc/7SFA-6FRA] (estimating that the United States suffered losses between $57 and $109 billion in 2016 due to cyberattacks); *see also* Clayton, *supra* note 11 (citing the importance of cybersecurity to various actors, including market participants and investors); Benjamin Dynkin & Barry Dynkin, *Derivative Liability in the Wake of a Cyber Attack*, 28 ALB. L.J. SCI. & TECH. 23, 24, 26 (2018) (highlighting the potential for derivative lawsuits in the aftermath of cybersecurity attacks). Cyberattacks implicate various forms of sensitive information; when companies are hacked, customer information, intellectual property, and financial data, among others, are compromised. COUNCIL OF ECON. ADVISERS, *supra*. The personal data of over two billion people—representing approximately two-thirds of online services users—has been compromised or stolen. MCAFEE, EXECUTIVE SUMMARY: THE ECONOMIC IMPACT OF CYBERCRIME—NO SLOWING DOWN 1 (2018), https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf [https://perma.cc/R8QM-8CJJ]. In 2018, while the global average cost to a business that experienced a data breach was $3.86 million, in the United States the average cost was more than double that figure. Niall McCarthy, *The Average Cost of a Data Breach Is Highest in the U.S.*, FORBES (July 13, 2018), https://www.forbes.com/sites/niallmccarthy/2018/07/13/the-average-cost-of-a-data-breach-is-highest-in-the-u-s-infographic/#424b92592f37 [https://perma.cc/J7VH-FMHD] (citing a 2018 IBM study on the cost of data breaches stating that cyberattacks in 2018 cost U.S. companies $7.91 million). The associated costs of cyberattacks, however, cannot all be easily quantified. *See* COUNCIL OF ECON. ADVISERS, *supra*, at 6 (highlighting the difficulty of quantifying costs such as damage to reputation and theft of intellectual property). Hence, cybersecurity is a pressing concern. *See* Erik Sherman, *U.S. CEOs Are More Worried About Cybersecurity Than a Possible Recession*, YAHOO! FINANCE (Jan. 17, 2019), https://finance.yahoo.com/news/u-ceos-more-worried-cybersecurity-131750112.html [https://perma.cc/YM34-CRBV] (discussing a survey of more than eight hundred chief executives officers (CEOs), in which CEOs of American companies cited cybersecurity as their greatest existential concern in 2019); *see also* Robert J. Jackson Jr., Comm'r, U.S. Sec. & Exch. Comm'n, Corporate Governance: On the Front Lines of America's Cyber War (Mar. 15, 2018), https://www.sec.gov/news/speech/speech-jackson-cybersecurity-2018-03-15#_ftnref3 [https://perma.cc/UWM5-MPWN] (citing cybersecurity as the most important problem facing today's companies). A survey in early 2018 revealed that more than two-thirds of corporate executives surveyed stated that cybersecurity presented a threat to their companies. Jackson, *supra*.

[143] *See* Newman, *supra* note 122 (describing the importance of cybersecurity to the SEC's regulatory initiatives in 2018 and emphasizing its 2018 cybersecurity disclosure guidance and enforcement actions against companies stemming from cybersecurity incidents).

yond the mandatory disclosure regime.[144] Section A discusses current arguments against the SEC's growing involvement in cybersecurity regulation.[145] Section B highlights the debate over the efficacy of the SEC's disclosure guidance.[146]

A. Should the SEC Regulate Cybersecurity?

The SEC's ability to regulate cybersecurity flows from its authority to regulate the securities industry and to carry out federal securities laws.[147] The role of the SEC is to ensure both the protection of investors and the integrity of exchanges by eliminating abusive conduct.[148] In furtherance of these goals, the SEC has begun to regulate cybersecurity because of cybersecurity's implications for the SEC's constituents.[149] In addition to detrimental financial consequences for affected companies, cybersecurity incidents also have the potential to break down the operations of the securities exchanges.[150] The risk of succumbing to a cybersecurity incident has become greater with the increased reliance on technology for business operations in the modern era.[151] To protect its constituents—reporting companies, investors, and the exchanges—from

---

[144] *See infra* notes 147–187 and accompanying text.

[145] *See infra* notes 147–164 and accompanying text.

[146] *See infra* notes 165–187 and accompanying text.

[147] *See, e.g.*, Securities Exchange Act of 1934 § 10(b), 15 U.S.C. § 78j(b) (2018) (vesting the SEC with authority to promulgate rules relating to unlawful deceptive practices in the securities exchanges); *see* Ernst & Ernst v. Hochfelder, 425 U.S. 185, 195 (1976) (describing the authority delegated by Congress to the SEC under the Acts to effectuate securities regulation); *see also* Commission Statement and Guidance on Public Company Cybersecurity Disclosure, 83 Fed. Reg. at 8168 (providing that, pursuant to the mandatory disclosure regime, public companies have a duty to disclose material cybersecurity risks). *See generally What We Do*, *supra* note 28.

[148] *See What We Do*, *supra* note 28 (identifying investor protection and ensuring fair and efficient exchanges as the mission of the SEC).

[149] *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosure, 83 Fed. Reg. 8166, 8166 (Feb. 26, 2018) (introducing interpretive guidance governing the disclosure of cybersecurity risks and incidents by public companies regulated by the SEC); Div. of Corp. Fin., *supra* note 12 (describing the Division of Corporation Finance's initial approach towards disclosure of cybersecurity incidents); *see also* Clayton, *supra* note 11 (articulating the approach of the SEC in initiating its cybersecurity regulatory efforts). *See generally Spotlight on Cybersecurity, the SEC and You*, U.S. SEC. & EXCHANGE COMMISSION, https://www.sec.gov/spotlight/cybersecurity [https://perma.cc/J9EH-3V5G] (outlining the SEC's approach to and recommendations regarding cybersecurity).

[150] *See* Clayton, *supra* note 11 (acknowledging a breach to the SEC's EDGAR system in 2016); *see also* DEPOSITORY TR. & CLEARING CORP., SYSTEMIC RISK BAROMETER: 2019 RISK FORECAST 1 (2018), http://www.dtcc.com/~/media/Files/Downloads/Press-Room/14590-Systemic-Risk-2018.pdf [https://perma.cc/2ZYZ-3UVK] (highlighting a survey in which cybersecurity was identified as the greatest risk to the global economy). For greater discussion of the economic implications of cybersecurity incidents, see *supra* note 142 and accompanying text.

[151] WORLD ECON. FORUM, THE GLOBAL RISKS REPORT 2018, at 14–15 (2018), http://www3.weforum.org/docs/WEF_GRR18_Report.pdf [https://perma.cc/L6JE-VPL7] (stating that the frequency of cybersecurity incidents nearly doubled between 2012 and 2017, and that cybercrime is projected to cost industries eight trillion dollars over the next five years).

these devastating consequences, the SEC turned its attention to cybersecurity risks and incidents.[152]

Another important reason for the SEC's activity in this space is the lack of uniform federal privacy laws and absence of comprehensive federal cybersecurity regulation in the United States.[153] Current cybersecurity regulation largely

---

[152] *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosure, 83 Fed. Reg. at 8166–67 (discussing the implications and cost of cybersecurity incidents—including damage to stock price, litigation costs, and higher premiums for insurance—and introducing clarification about a public company's obligations under the federal securities laws with respect to cybersecurity); Press Release, *supra* note 120.

[153] *See, e.g.*, Victoria Conrad, Note, *Digital Gold: Cybersecurity Regulations and Establishing the Free Trade of Big Data*, 10 WM. & MARY BUS. L. REV., 295, 315 (2018) (noting that the only standardized approach by the federal government vis-á-vis cybersecurity consists of policy coupled with a future intent to centralize cybersecurity regulation, but noting the plethora of approaches at the state level). In contrast to the approach in the United States, on April 14, 2016, the European Union Parliament enacted the General Data Protection Regulation (GDPR), which intended to standardize Europe's laws protecting data privacy. *See Data Protection in the EU*, EUROPEAN COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en [https://perma.cc/KRE5-ENJV] (discussing the enactment of the GDPR). The GDPR came into effect on May 25, 2018. *Id.* The GDPR applies to any company that (1) "processes personal data as part of the activities of one of its branches established in the EU," or (2) is "established outside the EU and is offering goods/services (paid or for free) or is monitoring the behaviour of individuals in the EU." *Who Does the Data Protection Law Apply To?*, EUROPEAN COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en [https://perma.cc/SW96-DPG4]. The GDPR applies regardless of whether the data processing takes place within or outside of the European Union. *Id.* Relevant to the topic of this Note, if a company covered by the GDPR experiences a cybersecurity incident, it must notify the appropriate authority within seventy-two hours of the breach, unless the incident is not likely to "risk . . . the rights and freedoms of natural persons." Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, 33. Similarly, the company must communicate the existence of the breach to the affected "data subject" when the incident is "likely to result in a high risk to the rights and freedoms of natural persons." *Id.* at 34. Failure to adhere to the provisions of the GDPR could result in "a range of sanctions, including suspension of activities and fines." *Sanctions*, EUROPEAN COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/sanctions_en [https://perma.cc/8GA2-USDM]. *See generally* JONES DAY, GENERAL DATA PROTECTION REGULATION GUIDE (2017), https://www.jonesday.com/files/upload/GDPR%20Pocket%20Guide%20A5%2004_17_18%20ENGLISH.pdf [https://perma.cc/3HPN-WVD3] (providing an overview of the GDPR and its implications for affected companies and individuals). Stemming from the 2018 breach, Marriott became the second company to face a potential financial penalty under the GDPR. *See Statement: Intention to Fine Marriott International, Inc More Than £99 Million Under GDPR for Data Breach*, INFO. COMMISSIONER'S OFF. (July 9, 2019), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/ [https://perma.cc/9LCT-VK42] (announcing an intention to fine Marriott approximately £99 million); *see also* Marriott Int'l, Inc., Exhibit 99 to Current Report (Form 8-K) (July 9, 2019) (disclosing the fine to Marriott investors). British Airways was the first company whose penalty under the GDPR was announced publicly. Kate O'Flaherty, *Marriott Faces $123 Million Fine for 2018 Mega-Breach*, FORBES (July 9, 2019), https://www.forbes.com/sites/kateoflahertyuk/2019/07/09/marriott-

consists of divergent approaches at the state level.[154] Because no single federal agency is by statute charged with carrying out cybersecurity regulation, the SEC has addressed cybersecurity concerns relevant to its regulatory jurisdiction.[155]

Some criticism, however, cautions that providing the SEC with information relating to cybersecurity may in fact be harmful.[156] In regulating cybersecurity, the SEC requires its constituents to hand over highly sensitive information.[157] The cybersecurity information a company discloses to the SEC could ultimately be used against the company if the SEC's own cybersecurity is compromised and the information is misappropriated by malicious actors.[158]

The SEC is not impenetrable—neither physically nor in cyberspace.[159] In September 2018, a report issued by the Government Accountability Office (GAO) found that the SEC had not adequately maintained constant monitoring of the security of its information technology systems.[160] The report stated that

---

faces-gdpr-fine-of-123-million/#5010a6924525 [https://perma.cc/NZ4B-K7AT] (detailing British Airways' £183 million penalty).

[154] *See, e.g.*, Conrad, *supra* note 153, at 316–17 (describing the divergent cybersecurity regulatory efforts at the state level and noting the significant compliance burden they impose on companies that operate across state lines). *See generally* Charlotte A. Tschider, *Experimenting with Privacy: Driving Efficiency Through a State-Informed Federal Data Breach Notification and Data Protection Law*, 18 TUL. J. TECH. & INTELL. PROP. 45 (2015) (discussing the patchwork regulatory efforts resulting from the state-by-state approach to data protection and data breach notification statutes).

[155] Ieuan Jolly, *Data Protection in the United States: Overview*, THOMSON REUTERS: PRACTICAL LAW (Oct. 1, 2018), https://us.practicallaw.thomsonreuters.com/6-502-0467 [https://perma.cc/LGR5-LJQW] (citing the absence of one central cybersecurity statute and describing the United States' regulatory efforts in this area as "a patchwork system of federal and state laws and regulations that can sometimes overlap, dovetail and contradict one another"); *see, e.g.*, Commission Statement and Guidance on Public Company Cybersecurity Disclosure, 83 Fed. Reg. at 8166 (presenting the SEC's most recent interpretive guidance regarding the disclosure obligations of public companies regarding cybersecurity incidents).

[156] *See* Selznick & LaMacchia, *supra* note 13, at 37 (arguing that the cybersecurity information the SEC requests from its regulated entities could be "too sensitive" given the SEC's own cybersecurity weaknesses).

[157] Commission Statement and Guidance on Public Company Cybersecurity Disclosure, 83 Fed. Reg. at 8169 (instructing public companies to disclose material information relating to cybersecurity, including "disclosure[s] that [are] tailored to their particular cybersecurity risks and incidents").

[158] *See* Press Release, *supra* note 119 (describing the 2016 breach of the SEC's EDGAR system, which generated over four million dollars in illegal trading profits for the individuals who allegedly breached the system). For further discussion of the 2016 breach of EDGAR, see *supra* note 119 and accompany text.

[159] *See* Selznick & LaMacchia, *supra* note 13, at 56–57 (discussing a 2014 report issued by the Government Accountability Office (GAO) identifying weaknesses in the SEC's security); Sarah N. Lynch, *U.S. SEC's Information Technology at Risk of Hacking—Report*, REUTERS (Apr. 17, 2014), https://www.reuters.com/article/sec-cybercrime-security-idUSL2N0N91GU20140417 [https://perma.cc/KDJ3-6CT4] (noting that the 2014 GAO report identified weaknesses in both the SEC's cybersecurity and physical security).

[160] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-18-622, HIGH-RISK SERIES: URGENT ACTIONS ARE NEEDED TO ADDRESS CYBERSECURITY CHALLENGES FACING THE NATION 62 (2018), https://www.gao.gov/assets/700/694355.pdf [https://perma.cc/P4AB-EE96] (stating that the SEC "did not

despite the GAO bringing this to the SEC's attention in the previous year, the SEC had yet to change its practices.[161] Considering whether the SEC should be regulating cybersecurity raises questions about the SEC's own level of cybersecurity protection.[162] Despite the fact that the SEC has reassured reporting companies that they are not required to be so detailed in disclosure so as to provide a "roadmap" of their cybersecurity efforts—lest the information fall into the hands of those who would misuse it—critics question the advisability of requiring companies to share any cybersecurity information at all.[163] Because cybersecurity information is inherently sensitive, the risk of an incident could increase if companies share information with an SEC that cannot guarantee that the information will not become compromised or misappropriated.[164]

B. If the SEC Is to Regulate Cybersecurity, Is Disclosure the Most Effective Way?

The SEC's foray into cybersecurity regulation begs the question of whether disclosure is the most effective means by which to regulate growing cybersecurity issues.[165] In recent years, the SEC has conducted examinations of cybersecurity policies and created the Cyber Unit within the Division of

always keep system security plans complete and accurate or fully implement continuous monitoring, as required by agency policy").

[161] *Id.* at 62–63. The report identified other government agencies with information technology systems and security deemed to be deficient. *See id.* at 63 (identifying weaknesses with the Internal Revenue Service, the Federal Deposit Insurance Corporation, and the Food and Drug Administration, among other agencies).

[162] *See* Francine McKenna, *SEC's Case Against Edgar Hackers Highlights Regulator's Own Cyber Weaknesses*, MARKETWATCH (Jan. 15, 2019), https://www.marketwatch.com/story/secs-case-against-edgar-hackers-highlights-regulators-own-cyber-weaknesses-2019-01-15 [https://perma.cc/K48J-W53S] (describing the breach of the SEC's EDGAR system and its implications for the SEC's own cybersecurity efforts).

[163] *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosure, 83 Fed. Reg. at 8169 (stating that SEC filers are not required to provide such great detail in cybersecurity disclosures so as to give a "roadmap" to would-be hackers); McKenna, *supra* note 162 (describing some criticism of the SEC's approach to cybersecurity regulation).

[164] *See* McKenna, *supra* note 162 (citing a former member of the SEC's Division of Enforcement who questions whether the SEC should permit companies to include material, nonpublic information in test filings with the SEC, in light of the increasing prevalence of cybersecurity incidents). In a recent statement discussing the ongoing enforcement action against the alleged perpetrators, Chairman of the SEC Jay Clayton acknowledged that the SEC faces many of the same cybersecurity risks as the entities it regulates, and acknowledged that "[n]o system can be entirely safe from a cyber intrusion." Jay Clayton, Chairman, U.S. Sec. & Exch. Comm'n, Statement on EDGAR Hacking Enforcement Action (Jan. 15, 2019), https://www.sec.gov/news/public-statement/statement-clayton-011519 [https://perma.cc/ZT4A-WQ8Y].

[165] *See* Selznick & LaMacchia, *supra* note 13, at 36–37 (describing various means of regulation by the SEC, including mandatory disclosure of cybersecurity-related information as well as cybersecurity examinations conduct by the SEC's Office of Compliance and Examinations).

Enforcement to combat cybersecurity abuses in the securities markets.[166] Consistent with the mandatory disclosure regime, however, the primary method through which the SEC has regulated cybersecurity is by requiring public companies to disclose cybersecurity risks and incidents in their SEC filings.[167] The SEC has affirmed that under the federal securities laws, public companies have a duty to disclose to investors all material information regarding cybersecurity risks and incidents.[168] Standard boilerplate language in these disclosures does not suffice; reporting companies must disclose in appropriate detail the specific cybersecurity risks to which the company is exposed, as well as any incidents to which it has succumbed.[169] In order to do so effectively, the SEC expects a public company to develop controls and procedures designed to discern cybersecurity risks and incidents, evaluate their effect on the company's operations, and asses their potential materiality.[170] To ensure timely and appropriate disclosure, the policies and procedures must also ensure that this information is reported to the correct company personnel.[171]

Proponents of the SEC's regulatory efforts in this area cite investor protection, one of the most commonly cited rationales for the mandatory disclosure regime, as an important justification for cybersecurity disclosure obligations.[172] An investor is better able to assess her investment in a particular re-

---

[166] *See* Press Release, *supra* note 120 (announcing the creation and purpose of the SEC's Cyber Unit); *see also Spotlight on Cybersecurity, the SEC and You*, *supra* note 149 (noting that cybersecurity is a major focus of an SEC examination). For more detailed discussion of the Cyber Unit within the SEC's Division of Enforcement, see *supra* notes 120–121 and accompanying text.

[167] *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosure, 83 Fed. Reg. at 8168–70 (discussing the rules promulgated under the federal securities law that do not explicitly mention cybersecurity but nonetheless compel disclosure of material cybersecurity risks and incidents).

[168] *See id.* at 8167 (instructing public companies to disclose to investors those cybersecurity risks and incidents that are material and to do so in a "timely fashion").

[169] *Id.* at 8169 (describing the materiality standard as it applies to cybersecurity issues and cautioning reporting companies to provide meaningful cybersecurity disclosure for investors, rather than boilerplate language); *see* Press Release, *supra* note 138 (stating that Yahoo! failed to disclose the breach to which it succumbed in 2014; instead it only disclosed that it faced a risk of cybersecurity incidents).

[170] *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosure, 83 Fed. Reg. at 8171 (discussing the cybersecurity disclosure controls and procedures that a public company is expected to maintain pursuant the federal securities laws). The SEC further provided that such policies and procedures seek to allow a reporting company to detect, assess for materiality, and make timely disclosure of cybersecurity risks and incidents. *Id.*

[171] *See id.* (noting that a public company's controls and procedures should aggregate and report cybersecurity-related information to the proper personnel within the company). In effect, the SEC is instructing boards and management to take more active roles in their companies' cybersecurity efforts. *See id.* (noting that policies should facilitate the sharing of cybersecurity-related information with "the appropriate personnel, including up the corporate ladder").

[172] *See* Chadbourne & Parke LLP v. Troice, 571 U.S. 377, 390 (2014) (citing investor protection as the goal of federal regulation); *Ernst & Ernst*, 425 U.S. at 195 (citing the protection of investors as the purpose of both the Securities Act and the Exchange Act); Morse et al., *supra* note 141, at 10

porting company when that company provides full and truthful disclosure of the cybersecurity risks and incidents it faces.[173] Moreover, given the financial consequences, among other implications, of cybersecurity incidents, these incidents are likely considered to be material.[174] Stated differently, an investor is likely to consider the existence of cybersecurity risks or incidents to be a significant factor when making an investment-related decision.[175]

There are, however, some criticisms of the SEC's mandatory disclosure approach to cybersecurity.[176] Although all SEC Commissioners unanimously approved the 2018 guidance, then-Commissioner Kara Stein stated that the guidance simply repeated much of the substance of the 2011 guidance.[177] Stein provided several examples of alternative steps the SEC could have taken, such as tailoring the new guidance to reflect relevant information the SEC had learned since its staff issued the 2011 guidance.[178] Likewise, then-SEC Commissioner Robert J. Jackson Jr. stated that the 2018 guidance merely recycles

(stating that information pertaining to cybersecurity is the kind of information about which investors would want to be informed). By providing investors with full and accurate disclosure, an investor is empowered to make an informed decision regarding her position in the company, improving market efficiency. *See, e.g.*, Mastronardi, *supra* note 10, at 343 (stating that the mandatory disclosure regime increases investors' access to accurate information, thereby protecting investors from exploitation).

[173] *See* Forrest E. Lind III, *Governing Cybersecurity: The SEC Enters the Ring*, 3 EMORY CORP. GOVERNANCE & ACCOUNTABILITY REV. 2032, 2035 (2016) (stating that disclosure of cybersecurity-related information enables investors to make informed decisions regarding their investments); Turk & Woody, *supra* note 32, at 969 nn.49, 52 (expounding upon the underlying premise of the mandatory disclosure regime).

[174] *See* Lind, *supra* note 173 (stating that cybersecurity risks and incidents are the type of information needed to assess accurately an investment opportunity and about which investors would want to be informed).

[175] *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosure, 83 Fed. Reg. at 8168 & n.32 (describing the SEC's standard of materiality for disclosures under the federal securities laws and its consistency with the materiality standard put forth by the Supreme Court in *TSC Industries, Inc. v. Northway*); *see also* TSC Indus., Inc. v. Northway, 426 U.S. 438, 449 (1976) (providing that a fact is material if a reasonable investor would either be significantly likely to consider it critical in making a decision about her investments, or would have considered it to change significantly the amount of information provided to the investor).

[176] *See* Selznick & LaMacchia, *supra* note 13, at 56–57 (arguing that the SEC's regulation of cybersecurity is problematic due to its own cyber-related vulnerabilities); Craig A. Newman, *When to Report a Cyberattack? For Companies, That's Still a Dilemma*, N.Y. TIMES (Mar. 5, 2018), https://www.nytimes.com/2018/03/05/business/dealbook/sec-cybersecurity-guidance.html [https://perma.cc/EDC7-CGS3] (describing the difficulties and tensions public companies experience when determining whether to disclose cybersecurity-related information and stating that the guidance does not help to balance the decisions of working with law enforcement and informing investors).

[177] Stein, *supra* note 16. Stein's term expired on January 2, 2019. *SEC Historical Summary of Chairmen and Commissioners*, U.S. SEC. & EXCHANGE COMMISSION, https://www.sec.gov/about/sechistoricalsummary.htm [https://perma.cc/RR7G-Y6P5].

[178] *See* Stein, *supra* note 16 (offering examples of other regulatory initiatives the SEC could have undertaken).

the content of its predecessor and that cybersecurity regulation must instead be extended further.[179]

Another criticism is that the SEC's guidance does little to clarify *when* a reporting company's obligations with respect to cybersecurity arise under the mandatory disclosure regime.[180] Although the SEC's guidance stresses the need for "timely" disclosure, it does not expand upon what makes disclosure "timely."[181] The 2018 guidance is seen as too general, and leaves reporting companies wondering whether disclosure of a cybersecurity incident can wait until the end of the quarter, whether it can wait until the end of the fiscal year, or whether it must be made immediately in a Current Report Form 8-K.[182]

Lastly, although the guidance asserts that public companies are not required to provide such detail in their disclosures that their cybersecurity efforts could be compromised, critics question the feasibility of complying with the disclosure requirements *without* compromising a company's cybersecurity.[183] For example, a company that discloses a cybersecurity risk particular to its

---

[179] *See* Robert J. Jackson Jr., Comm'r, U.S. Sec. & Exch. Comm'n, Statement on Commission Statement and Guidance on Public Company Cybersecurity Disclosures (Feb. 21, 2018), https://www.sec.gov/news/public-statement/statement-jackson-2018-02-21 [https://perma.cc/2Q7K-4K4D] ("I reluctantly support today's guidance in the hope that it is just the first step toward defeating those who would use technology to threaten our economy."). In early 2020, Commissioner Jackson announced his exit from the SEC. Paul Kiernan, *SEC Commissioner Jackson Resigns to Return to Law School Teaching Position*, WALL ST. J. (Jan. 16, 2020), https://www.wsj.com/articles/sec-commissioner-jackson-resigns-to-return-to-law-school-teaching-position-11579183208 [https://perma.cc/QG5G-2ZTH].

[180] *See* COUNCIL OF ECON. ADVISERS, *supra* note 142, at 31 (discussing concerns that the SEC's 2011 guidance does not enable firms to determine what quantity of information to provide in disclosure, and hence does not resolve the information imbalance the mandatory disclosure regime seeks to address); Newman, *supra* note 176 (asserting that the SEC's 2018 guidance does little to help reporting companies ascertain when to disclose a cybersecurity incident). The Council of Economic Advisers further discussed the dearth of disclosures of cybersecurity incidents and the policy implications of this lack of data. COUNCIL OF ECON. ADVISERS, *supra* note 142, at 32.

[181] *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosure, 83 Fed. Reg. at 8167–72 (repeatedly asserting the need for public companies to make "timely" disclosure of material cybersecurity-related information, but failing to further clarify any timeframe); Monica Pal, *Why Don't Companies Come Clean After a Data Breach?*, SILICON VALLEY BUS. J. (Feb. 10, 2019), https://www.bizjournals.com/sanjose/news/2019/02/06/4iq-ceo-monica-pal-data-breaches-op-ed.html [https://perma.cc/AV96-44C7] (arguing that public companies face a choice between making disclosure soon after a breach, when they may not have all the necessary information, and waiting to disclose, resulting in more accurate disclosure).

[182] *See* COUNCIL OF ECON. ADVISERS, *supra* note 142, at 31 (citing concerns that the SEC's guidance is "too general"); Newman, *supra* note 176 (stating that the SEC's new guidance neither fully appreciates nor clarifies the conflict public companies experience when faced with the question of whether to disclose cybersecurity incidents).

[183] *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosure, 83 Fed. Reg. at 8169 (stating that a reporting company is not required in its disclosures with the SEC to offer such granularity as to offer a "roadmap" of how to exploit the company's cybersecurity vulnerabilities); Morse et al., *supra* note 141, at 9–10 (discussing the cybersecurity implications inherent in a company's compliance with disclosures under SEC cybersecurity guidance).

business is, in effect, disclosing that an investment with the company is risky because of cybersecurity concerns.[184] Moreover, even if the company does not provide a roadmap to those who would potentially use the information for nefarious purposes, disclosure of cybersecurity risks is a signal to the public that the company is vulnerable, and could succumb to an attack.[185] Some scholars note that even a generalized disclosure of cybersecurity concerns—which the SEC stated in its guidance is not permitted—could expose the company to further risk.[186] The more information a company discloses to investors, commentators assert, the greater the chance that information could ultimately find its way into the hands of those who will exploit it: hackers.[187]

III. The SEC Must Further Explain, Rather Than Repeat, Its Requirements Relating to Cybersecurity Disclosure

Because of the consequences for individual reporting companies and the securities markets at large, the SEC is properly taking a stance on the issue of cybersecurity.[188] In initiating regulatory efforts in this area, the SEC has taken another step to further its mission of investor protection and market regulation.[189] Cybersecurity regulation furthers investor protection because, through the mandatory disclosure regime upon which federal securities regulation is premised, the SEC ensures investors are appropriately informed about the cybersecurity risks of the companies in which they invest.[190] The SEC imple-

---

[184] Morse et al., *supra* note 141, at 9.

[185] *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosure, 83 Fed. Reg. at 8169 (attempting to qualify the level of detail required to fulfill a company's reporting obligations with respect to cybersecurity); Morse et al., *supra* note 141, at 9–10 (discussing the message of vulnerability that a company presents when making disclosure relating to cybersecurity).

[186] *See* Howard M. Privette et al., *The SEC Guidance on Cybersecurity Measures for Public Companies*, L.A. LAW., Sept. 2014, at 14, 15 (noting that former SEC-commissioner Roberta Karmel suggested that disclosure of cybersecurity risks at all is contrary to the public interest by bringing those issues to light for exploitation by hackers). In effect, disclosure of cybersecurity-related issues could expose the company to greater risk. *See id.* at 17 (discussing both the risk that disclosure will exacerbate future cyberattacks against the company and the risk that such disclosure will generate additional shareholder derivative litigation). For greater discussion of derivative litigation, see *supra* note 141 and accompanying text.

[187] *See* Privette et al., *supra* note 186, at 14 (describing the conundrum companies face: investors are likely interested in receiving disclosure of cybersecurity incidents and risks, but providing disclosure in too much detail would reveal vulnerabilities of the company that may end up in the hands of hackers).

[188] *See* Clayton, *supra* note 11 (asserting that investors ultimately internalize much of the cost of cybersecurity incidents).

[189] *See* Selznick & LaMacchia, *supra* note 13, at 61 (describing how the SEC furthers its mission of market regulation and investor protection in its regulation of cybersecurity).

[190] *See id.* (asserting that the required disclosure of only material cybersecurity incidents ensures that investors obtain the information they need without compromising a company's security); Thompson & Sale, *supra* note 28, at 869–70 (stating that federal securities regulation aims to correct the

ments market regulation by ridding cybersecurity-related abuses from the market—in particular through the Division of Enforcement's Cyber Unit.[191]

Although the SEC is rightly taking strides to address cybersecurity concerns, to be effective it must: (1) resolve its own cybersecurity flaws; and (2) further clarify the scope of the disclosure obligations by explaining what makes a cybersecurity incident "material" and what constitutes "timely" disclosure.[192] Section A argues that the SEC must shore up its own cybersecurity measures to effectively regulate the cybersecurity of its reporting companies.[193] Section B asserts that the SEC must further explain, and not simply reiterate, the disclosure requirements pertaining to cybersecurity.[194]

A. Flaws in the SEC's Own Cybersecurity Prevent It from Effectively Ensuring the Cybersecurity of Its Regulated Entities

Recent reports have highlighted the flaws in the SEC's approach to its own cybersecurity.[195] Not only have the SEC's own databases succumbed to cybersecurity incidents, but the GAO has labeled the SEC's cybersecurity measures as inadequate.[196] Although the SEC is properly taking a stance in this area, the SEC will only exacerbate current cybersecurity concerns if its own cybersecurity is compromised again.[197] A company's risk of experiencing a cyberattack is amplified, rather than decreased, by reporting its own cyberse-

---

informational asymmetry between companies and investors by requiring companies to make substantial disclosures to investors through SEC filings).

[191] *See* Press Release, *supra* note 120 (announcing that the Cyber Unit will be tasked with ridding the market of cyber-related misconduct, such as "[h]acking to obtain material nonpublic information" or "[c]yber-related threats to trading platforms and other critical market infrastructure").

[192] *See infra* notes 195–215 and accompanying text.

[193] *See infra* notes 195–201 and accompanying text.

[194] *See infra* notes 202–215 and accompanying text.

[195] *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 160, at 62–63 (discussing ongoing flaws with the cybersecurity measures employed by the SEC); Selznick & LaMacchia, *supra* note 13, at 56–57 (describing a 2014 GAO report that highlighted two overarching areas in which the SEC's cybersecurity measures are lacking: "(1) maintenance and monitoring of configuration baseline standards; and (2) implementation of password setting and network service standards"). In 2018, four years after the 2014 report, another GAO report asserted that the SEC still had some inadequate security measures, even though the GAO had previously brought these deficiencies to the SEC's attention. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 160, at 62–63.

[196] *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 160, at 62–63 (noting that some of the cybersecurity methods deployed by the SEC are deficient, despite earlier warnings from the GAO about such deficiencies); Press Release, *supra* note 119 (announcing that hackers infiltrated the SEC's EDGAR system in 2016).

[197] *See* Press Release, *supra* note 119 (describing the 2016 hack of EDGAR). The hack of the SEC's EDGAR system, for example, enabled the hacking parties to trade on material information that was submitted to the SEC but not yet made public. *Id.* In total, the individuals amassed more than four million dollars in unlawful trading profits. *Id.* This abuse is exactly of the type that the SEC seeks to prevent. *See What We Do*, *supra* note 28 (stating that "protecting against fraud" is a responsibility of SEC).

curity risks to the SEC because of the SEC's imperfect cybersecurity systems.[198] If the sensitive cybersecurity-related information given to the SEC—whether through disclosure or examinations—is misappropriated, the SEC's efficacy in keeping such information secure and out of the wrong hands is thwarted.[199] Consequently, if the SEC is going to require public companies to hand over highly sensitive information, the SEC must practice what it preaches.[200] Moving forward, the SEC must make its own cybersecurity a priority, particularly in light of recent well-publicized breaches to its own systems.[201]

B. The SEC Must Further Clarify Reporting Companies' Disclosure Obligations of Cybersecurity Risks and Incidents

To date, the SEC has implemented its regulation of cybersecurity largely through its mandatory disclosure regime.[202] The SEC has asserted that the entities it regulates must disclose material cybersecurity risks and incidents, and must do so in a timely fashion.[203] The SEC has not, however, clearly articulated what makes a cybersecurity risk or incident material.[204] Consequently, public companies often disclose copious amounts of information in their filings, in some instances burying information that is likely to be material under infor-

---

[198] *See* Selznick & LaMacchia, *supra* note 13, at 61 ("Publicly reporting cybersecurity management policy and storing sensitive examination information in insecure SEC technology infrastructure increase the risk of cyberattacks.").

[199] *See id.* (arguing that reporting cybersecurity and other sensitive information to the SEC to then be stored in unsecure systems exacerbates the risk of succumbing to cybersecurity incidents).

[200] *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 160, at 3 (stating that the report pinpoints changes that federal agencies, including the SEC, must implement to strengthen the agencies' cybersecurity profiles); Selznick & LaMacchia, *supra* note 13, at 56–57 (describing the SEC's cybersecurity shortcomings and arguing that the SEC should take steps to protect the sensitive information that it, by virtue of its work, must collect).

[201] *See* Press Release, *supra* note 119 (noting that individuals who successfully breached EDGAR garnered more than four million dollars in illegal trading profits).

[202] *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Exchange Act Release No. 33-10459, 83 Fed. Reg. 8166, 8166 (Feb. 26, 2018) (representing the SEC's most recent guidance on the reporting requirements regarding cybersecurity imposed on public companies by the federal securities laws and the regulations promulgated thereunder).

[203] *Id.* at 8168 (asserting that public companies must disclose to investors those material cybersecurity risks and incidents, even though the requisite disclosure requirements do not speak directly to cybersecurity-related issues).

[204] *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. at 8168–69 (articulating the standard of materiality and how it relates to cybersecurity-related issues). Although the SEC mentioned the well-known standard of materiality—if a reasonable investor is substantially likely to view the information as significant in making an investment-related determination—the SEC did not provide examples of the kinds of incidents that would satisfy the standard. *Id.* The SEC identified numerous factors that a company should consider in deciding whether an incident is material, but provided no concrete examples of those factors. *See id.* (stating that factors such as "nature, extent, and potential magnitude" influence whether a cybersecurity incident is material).

mation that is less pertinent.[205] Over-disclosing information to investors renders ineffective the investor-protection centered model of securities regulation because, by inundating investors with information, they are unable to discern what information matters to their investment decisions.[206] The SEC, therefore, must provide more clarity about what types of events, and at what scale, meet the materiality standard and, therefore, must be disclosed in SEC filings.[207] With a better understanding of what incidents and risks are material, public companies can more clearly disclose them to investors, thereby furthering the aims of the federal securities laws.[208]

Moreover, the SEC has not provided a clear timeframe to which a public company is expected to adhere in disclosing cybersecurity concerns.[209] A clearly laid out timeframe would have helped to prevent Marriott from waiting over two months to disclose a large cybersecurity breach of one of its databases.[210] Likewise, it would provide all companies with a clear yardstick by which to measure the timeliness of their disclosures.[211] Investors would receive more

---

[205] *See* Selznick & LaMacchia, *supra* note 13, at 55 (quoting Am. Int'l Grp., Inc., Annual Report (Form 10-K) (Feb. 15, 2013)) (highlighting one example of disclosure in which a company stated that "[l]ike other global companies, we have, from time to time, experienced threats to our data and systems, including malware and computer virus attacks, unauthorized access, systems failures and disruptions," and arguing that an investor is unable to discern the true and relevant meaning of such disclosure).

[206] *See* Mastronardi, *supra* note 10, at 344 (describing a common refrain that imposing too many disclosure obligations upon companies may inevitably overwhelm investors with so much information that they will be unable to determine the relevancy of the provided information).

[207] *See* Newman, *supra* note 176 (critiquing the SEC's 2018 guidance for doing little to help public companies sort through the "conflicting demands" implicated by cybersecurity incidents: remaining discreet about cybersecurity incidents in order to cooperate with the law enforcement officials tasked with investigating them, while also maintaining the company's obligations to disclose material information to investors).

[208] *See* Shelby, *supra* note 33 (stating that the purpose of investor protection underlying the federal securities laws is furthered by requiring public companies to disclose information pertaining to numerous areas of the companies' businesses, thereby preventing investor exploitation and other abusive practices); Newman, *supra* note 176 (suggesting that a lack of clarity and guidance from the SEC could represent why so few companies have disclosed cybersecurity incidents in filings with the SEC).

[209] *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. at 8167 (confirming that companies have an obligation to disclose cybersecurity risks and incidents in a "timely fashion"). In the 2018 guidance, the SEC repeatedly asserts the need for "timely" disclosure, but does not provide further explanation of what satisfies this requirement. *See id.* at 8167–72 (providing no clarification on what constitutes "timely" disclosure); Pal, *supra* note 181 (asserting that the SEC's 2018 guidance forces companies to balance prompt disclosure with correct disclosure).

[210] *See* Marriott Int'l, Inc., Current Report (Form 8-K) (Nov. 30, 2018) (representing the first disclosure Marriott made to investors in November 2018 regarding the cybersecurity incident it discovered in September 2018, representing a delay of more than two months).

[211] *See* Rajgopal & Gezer, *supra* note 6 (noting that the lack of specificity in the SEC's current cybersecurity disclosure guidance enables companies to delay disclosure of cybersecurity risks and incidents).

timely and accurate information as to the cybersecurity risks and incidents faced by the companies in which they are invested.[212] Moreover, given that the size and scope of an incident may not be immediately apparent, a timeframe is particularly important because, to date, there has been a wide variation of how swift, or slow, companies are to disclose cybersecurity incidents.[213]

Consequently, although the SEC has emphasized the need for disclosure—an important first step in requiring public companies to take seriously the cybersecurity threats they face—some aspects of the SEC's regulatory efforts require further clarification.[214] To ensure adequate market regulation and investor protection, the SEC must help companies help themselves by specifying when to disclose cybersecurity risks and incidents and what information to provide.[215]

CONCLUSION

Cybersecurity is a grave threat to publicly-traded companies and the economy at large. Consequently, the SEC has turned its regulatory attention to issues pertaining to cybersecurity. Pursuant to its authority to carry out the federal securities laws, which seek to protect investors and regulate the securities exchanges, the SEC has carried out cybersecurity regulation primarily through its mandatory disclosure regime. Although no SEC requirements speak specifically to cybersecurity, SEC guidance issued in 2018 explains that public companies nonetheless must disclose in a timely fashion those cybersecurity risks and incidents that are material to investors. The substance of this guidance, however, merely parroted statements from 2011 guidance issued by the SEC's Division of Corporation Finance and left companies unsure of their disclosure obligations.

---

[212] *See id.* (asserting that greater clarity in the disclosure obligations would ensure companies take such risks seriously and disclose them as needed to investors).

[213] *See* Pal, *supra* note 181 (providing as an example Facebook's announcement that some fifty million user accounts had been compromised three days after the hack occurred, when the company had only just commenced an investigation). Although Facebook later provided updates regarding the breach, stating that it affected approximately twenty million fewer users than initially estimated, it also revealed that the stolen information was more personal than initially believed. Mike Isaac, *Facebook Hack Included Search History and Location Data of Millions*, N.Y. TIMES (Oct. 12, 2018), https://www.nytimes.com/2018/10/12/technology/facebook-hack-investigation.html [https://perma.cc/372S-MMTX]. In its 2018 guidance, the SEC acknowledged that later updates to an initial disclosure of a cybersecurity incident may be necessary to account for information learned after the disclosure. *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. at 8169 (instructing reporting companies to assess whether updates to previously issued disclosure are needed, particularly when a cybersecurity incident is being investigated).

[214] *See* Jackson, *supra* note 142 (stating that companies that succumbed to cybersecurity incidents in 2017 opted not to file a Form 8-K in over ninety-seven percent of circumstances, and noting that he has urged the SEC to put forth new obligations regarding cybersecurity disclosure for Form 8-Ks).

[215] *See* Stein, *supra* note 16 (stating that the SEC's 2018 guidance simply parroted positions put forth in 2011 and pointing to other, more forward-looking actions the SEC could have taken with respect to cybersecurity disclosure).

Although the SEC has appropriately focused on cybersecurity given its significant implications, to be truly effective in the space the SEC must take two steps. First, the SEC must strengthen its own cybersecurity: requesting cybersecurity information from regulated entities should not, as is currently the case, increase risk that those entities will be exposed to cybersecurity threats. Second, the SEC must provide greater explanation of what makes a cybersecurity incident material—and thus worthy of disclosure—and what constitutes "timely" disclosure of cybersecurity incidents. Only with further clarity can the SEC achieve meaningful regulation in the cybersecurity space.

REBECCA RABINOWITZ