Note

Material Breach, Material Disclosure

*Tash Bottum**

INTRODUCTION

On September 7, 2017, Equifax announced that its servers had been breached, compromising the personal financial information of as many as 143 million Americans.[1] On that day, the Equifax stock was trading at $142.72.[2] In the week following Equifax's announcement, the stock price fell over thirty-three percent to $92.98.[3] Equifax is a credit reporting agency that compiles and sells credit reports comprised of information regarding an individual's financial history.[4] The company's database includes information concerning over 820 million consumers, over 91 million businesses, and the employees of over 7100 employers.[5] This breach damaged not only the consumers, but also the company's investors[6] who, at the time, owned over 120 million outstanding shares.[7] As the details of the hack emerged,

* J.D. Candidate 2019, University of Minnesota Law School. Thank you to Professor Prentiss Cox and Professor John Matheson for their thoughtful comments and guidance throughout this process. I would also like to thank the editors and staffers of the Minnesota Law Review for their careful and considerate edits. Thanks also to JGS + P, T, Q, G, S always.

1. *See* Thomas Fox-Brewster, *A Brief History of Equifax Security Fails*, FORBES (Sept. 8, 2017), https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#5ddff05d677c.

2. *Equifax, Inc.*, NYSE, https://www.nyse.com/quote/XXXX:EFX (last visited Mar. 10, 2019).

3. *Id.*

4. *See What Is a Credit Reporting Company?*, CFPB, https://www.consumerfinance.gov/ask-cfpb/what-is-a-credit-reporting-company-en-1251 (last updated May 25, 2017).

5. *See* Press Release, Equifax, Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes (Sept. 15, 2017), https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832.

6. For the purposes of this Note, "investor" or "investors" refers to a company's shareholders.

7. *See Equifax Shares Outstanding*, Y CHARTS, https://ycharts.com/companies/EFX/shares_outstanding (last updated Oct. 31, 2017).

Equifax's ethics and conduct became increasingly concerning to both the company's investors and the general public.

The untimeliness of Equifax's response—a critical component of data breach investigations—deepened these concerns.[8] Equifax first discovered the data breach on July 29, 2017.[9] However, the roots of this story trace back further. On March 8, 2017, security researchers at Cisco Systems, Inc. discovered a vulnerability in the Apache software used by Equifax.[10] Apache Software Foundation issued a patch to cure this vulnerability, and instructed companies to take necessary efforts to protect their systems.[11] On May 13, hackers first accessed sensitive information within Equifax's databases.[12] The hackers entered through the same vulnerability that the Apache-issued patch was intended to repair.[13] When Equifax discovered the breach, they patched the vulnerability,[14] but at that point, the damage had been done.

From July 29 until September 7, Equifax internally reviewed the breach and enlisted an independent cybersecurity firm, Mandiant, to assist in determining "the scope of the intrusion, including the specific data impacted."[15] Thus, it was not until forty days after Equifax first discovered the breach that the company disclosed the event to the public and to its investors.

During this forty-day delay, company executives within Equifax sold nearly $2 million worth of shares.[16] Regulatory fil-

8. *See* Stephanie Yonekura et al., *Mitigating and Investigating a Cybersecurity Incident*, GLOBAL INVESTIGATIONS REV. (Aug. 8, 2016), https://globalinvestigationsreview.com/insight/the-investigations-review-of-the-americas-2017/1067470/mitigating-and-investigating-a-cybersecurity-incident (explaining that the date that the incident was discovered, confirmed, and disclosed will have an impact on whether the company's response will be perceived as reasonable).

9. *See* Press Release, Equifax, *supra* note 5 (stating that on July 29, 2017, the company first detected suspicious activity on its servers).

10. *See* AnnaMaria Andriotis & Robert McMillan, *Hackers Entered Equifax Systems in March*, WALL ST. J. (Sept. 20, 2017), https://www.wsj.com/articles/hackers-entered-equifax-systems-in-march-1505943617.

11. *See id.*

12. *See id.*

13. Lily Hay Newman, *Equifax Officially Has No Excuse*, WIRED (Sept. 14, 2017), https://www.wired.com/story/equifax-breach-no-excuse/.

14. *See* Press Release, Equifax, *supra* note 5.

15. *Id.*

16. *See* AnnaMaria Andriotis, *Equifax Special Committee Clears Executives on Trades Before Breach Disclosure*, WALL ST. J. (Nov. 3, 2017), https://www

ings show that Chief Financial Officer, John Gamble; U.S. Information Solutions President, Joseph Loughran; and Workforce Solutions President, Rodolfo Ploder; completed stock sales on August 1 and August 2, totaling roughly $1.8 million worth of shares.[17] These transactions may not have been planned, as they were not listed on the company's scheduled trading plan.[18] Equifax—as well as a committee of the company's board of directors assembled to investigate these trades—stated the executives were unaware of the breach at the time of the trades.[19] Later investigations revealed that an additional executive—the now-former Chief Information Officer, Jun Ying—sold nearly one million shares after learning of the breach.[20] Ying remains the only executive charged with insider trading in connection with this breach.[21] Nonetheless, all of the executives' trades mitigated their financial harm, as the trades occurred in the wake of a breach which would later damage the remainder of the company's investors, large and small.

The Equifax breach is believed to be "one of the most significant data breaches given the scope of the information disclosed"[22] and the resulting damage to consumers and investors.[23]

.wsj.com/articles/equifax-special-committee-clears-executives-on-trades-before-breach-disclosure-1509715006.

17. *Id.*

18. *See* Alina Selyukh, *3 Equifax Executives Sold Stock Days After Hack That Wasn't Disclosed for a Month*, NPR (Sept. 8, 2017), https://www.npr.org/sections/thetwo-way/2017/09/08/549434187/3-equifax-executives-sold-stock-days-after-hack-that-wasnt-disclosed-for-a-month. A scheduled trading plan establishes pre-planned buying and selling of shares for a certain period of time. *See* JAMES R. TANENBAUM & BRIAN HIRSHBERG, MORRISON & FOERSTER LLP, FREQUENTLY ASKED QUESTIONS ABOUT RULE 10B5-1 PLANS 2 (2017). These plans are "especially useful" for insiders presumed to have nonpublic information, "such as officers, directors and other affiliates," and must be submitted in accordance with federal regulations. *Id.*

19. *See* Andriotis, *supra* note 16 (describing the committee's investigation and findings); *see also* Press Release, Equifax, Equifax Board Releases Findings of Special Committee Regarding Stock Sale by Executives (Nov. 3, 2017), https://investor.equifax.com/news-and-events/news/2017/11-03-2017-124511096.

20. *See* Stacy Cowley, *Ex-Equifax Executive Charged with Insider Trading Tied to '17 Breach*, N.Y. TIMES (Mar. 14, 2018), https://www.nytimes.com/2018/03/14/business/equifax-executive-insider-trading.html.

21. *Id.*

22. Andriotis & McMillan, *supra* note 10.

23. *See generally The Equifax Breach: An Overview*, CYBERWIRE NEWS, https://www.thecyberwire.com/articles/the-equifax-breach-an-overview.html (last updated Sept. 20, 2017) (stating that while the Equifax breach is not the largest to have occurred, "it may be among the most damaging in effect").

Following Equifax's September 7 announcement, public attention has focused predominantly on consumer harm, demonstrated, for example, by a fifty-state class action lawsuit alleging, among other things, that Equifax delayed informing consumers about the breach, thereby preventing them from mitigating the impending damage.[24] This Note shifts the focus to the company's shareholders—a group of individuals who entrusted Equifax with their money, and whose investments must pay for the damage the company caused. As of the time of this writing, Equifax's stock price has yet to recover to the preannouncement price.[25] Thus, the shareholders continue to be harmed. Regardless of whether the extent of such harm could have been mitigated, the damage resulting from the Equifax data breach is material.

While Equifax stands in the spotlight, it is not alone in its misfortune. In today's age of technology, companies dedicate vast resources to protecting incredible amounts of data and the focus on cybersecurity is rapidly increasing in all industries.[26] This focus, in large part, is a reflection of the risk that content data breaches present. For the purposes of this Note, a "content data breach" is defined as a data breach that has compromised at least 1000 records containing consumers' personally identifiable information.[27] As the Equifax content data breach demonstrates, this type of breach negatively impacts the company's stock price, and in turn, its investors.[28] These harms then trigger federal law.

24. *See, e.g.*, *id.* (discussing the implications of this breach on individuals' privacy); Kenneth R. Harney, *Data Breach at Equifax Prompts a National Class-Action Suit*, WASH. POST (Nov. 22, 2017), https://www.washingtonpost.com/realestate/data-breach-at-equifax-prompts-a-national-class-action-suit/2017/11/20/28654778-ce19-11e7-a1a3-0d1e45a6de3d_story.html?noredirect=on&utm_term=.38df7b6f9a3a (describing the lawsuit); Adam Shell, *Equifax Data Breach: Number of Victims May Never Be Known*, USA TODAY (Sept. 17, 2017), https://www.usatoday.com/story/money/2017/09/17/equifax-data-breach-number-victims-may-never-known/670618001 ("Countless Americans will no doubt suffer financial harm from the Equifax data breach.").

25. *See Equifax, Inc.*, *supra* note 2 (providing a real-time value of the stock).

26. *See infra* note 178 and accompanying text.

27. *See* discussion *infra* Part III.A. This definition borrows its numeric threshold from a Ponemon Institute study that examines data breaches. PONEMON INST., 2017 COST OF DATA BREACH STUDY 2 (2017) [hereinafter PONEMON STUDY]; *see also infra* notes 217–18 and accompanying text.

28. *See infra* Part III.B.

Corporate disclosure law requires companies to report certain types of events on a current basis.[29] The Securities and Exchange Commission (SEC) disclosure regulations are currently governed by a vague standard of materiality that fails to adequately guide companies in determining whether to disclose a breach.[30] While often beneficial,[31] the discretion that the materiality standard allows is inappropriate as it applies to reporting content data breaches. Disclosure law aims to promote transparency, enhance informed investments, and protect investors.[32] The materiality standard harms investors by decreasing corporate transparency. A breach harms investors by decreasing the share price. These harms offend the purposes of federal disclosure law.[33] Moreover, the rate and effects of data breaches has risen at an alarming rate, reaching a level that demands regulatory attention.[34] This Note proposes a new rule in lieu of applying a standard to reporting content data breaches. This new rule will clarify the existing ambiguity, requiring disclosure where the standard simply recommends disclosure. The Note argues that companies must disclose content data breaches within four days of discovery by means of the SEC's 8-K disclosure form—specifically, Item 2.06: Material Impairments.[35]

This Note proceeds as follows. Part I describes the recent boom of data breaches and a breach's potential effects and costs before tracing the origin of SEC disclosure requirements, the purpose of such requirements, and the development of the SEC framework relating to corporate disclosures. This Part also sets forth the most common standard for materiality in corporate disclosure law. Part II discusses the distinction between a standard and a rule, identifies the use of standards and rules in the context of corporate disclosure law, and proposes that content data breaches should be subject to a rule—rather than a standard—of materiality. This Part describes the immediate justifications of subjecting content data breaches to a bright-line rule that requires four-day disclosure through the SEC's Form 8-K. Finally, Part III explores the particulars of the proposed rule and its benefits and demonstrates that mandatory disclosure satisfies the

29. *See infra* Part I.B.
30. *See infra* Part III.C.
31. *See infra* Part I.D.
32. *See infra* Part I.A.
33. *See infra* Part III.B.
34. *See infra* Part II.C.
35. SEC, CURRENT REPORT (FORM 8-K), at 2 (2018) [hereinafter FORM 8-K].

original purposes of corporate disclosure law. Finally, this Part addresses the most prominent critique of this rule-based approach—the speculative nature of content data breaches, and the resulting difficulty in precise reporting—before concluding.

I. DATA BREACHES AND THE HISTORY OF SEC DISCLOSURE LAW

Content data breaches are a relatively new phenomenon and have recently gained widespread attention.[36] Company disclosure requirements, on the other hand, were established early on in disclosure law and are a central consideration of corporations today. This Part traces the recent upsurge in data breaches and the effects that a breach can have on a company. Next, it traces the enactment and development of SEC-required disclosures, the purposes that Congress and the SEC intended to protect through the relevant legislation, regulations, and amendments, and finally, the touchstone materiality standard used throughout corporate disclosure law.

A. THE RISE AND EFFECTS OF DATA BREACHES

Regulations governing corporate disclosures have been dynamic, aiming to serve the purposes of the Exchange Act, subsequent legislation, shifting shareholder interests, and market developments. The rise of technology, and electronically stored information (ESI) in recent years is a critical market change, presenting new threats and risks to companies of all sizes.[37] One such threat is a content data breach,[38] such as the Equifax data breach that was described in the Introduction. The number of reported breaches has increased at an alarming rate since the early 2000s,[39] with over 1000 breaches tracked in 2016 alone—a

36. *See, e.g.*, Juliana De Groot, *The History of Data Breaches*, DIGITAL GUARDIAN: DATAINSIDER (Jan. 3, 2019), https://digitalguardian.com/blog/history-data-breaches (stating that the frequency of publicly-disclosed data breaches increased in the 1980s, with public awareness beginning to rise in the early 2000s).

37. *See, e.g.*, De Groot, *supra* note 36 (explaining that the exponential growth of ESI provides a greater opportunity for cyber criminals to gain access through a breach).

38. *See Data Breach*, TREND MICRO, https://www.trendmicro.com/vinfo/us/security/definition/data-breach (last visited Mar. 10, 2019) (defining a data breach as "an incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner").

39. *See* De Groot, *supra* note 36. (noting an increase from 157 breaches reported in 2005 to 783 breaches in 2014).

forty percent increase over the previous year's number.[40] Data breaches have short-term and long-term effects, leaving a path of destruction in their wake.

Recent studies have demonstrated that data breaches negatively impact the stock share price of a company at the moment of public announcement with years of lasting effects.[41] In 2017, Comparitech conducted a study focusing on Wall Street's reaction to a data breach, identifying twenty-four previously breached companies, including Apple, Adobe Systems, eBay, Home Depot, JPMorgan, LinkedIn, Target, and Yahoo.[42] Comparitech examined each of the company's share prices prior to and after its public announcement of the incident, finding that a data breach has more of a long-term effect than an immediate one.[43] The companies' share prices only fell about 0.5% on average immediately following a breach.[44] Three years after the breach, however, the stocks had dropped 41.6% in comparison to the NASDAQ market performance.[45] Comparitech's study also

40. *See Data Breaches Increase 40 Percent in 2016, Finds New Report from Identity Theft Resource Center and CyberScout*, IDENTITY THEFT RESOURCE CTR., http://www.idtheftcenter.org/2016databreaches (Jan. 19, 2017) (noting 1091 reported breaches in 2016, as compared to 780 in 2015).

41. *See* Marc Butler, *Data Breaches Have Measurable Impact on Long-Term Stock Prices*, INTELLIGIZE (July 20, 2017), https://www.intelligize.com/data-breaches-measurable-impact-long-term-stock-prices (arguing that new research and studies show that "there is indeed a measurable impact [of data breaches] on short- and long-term stock value"). *But see* Elena Kvochko & Rajiv Pant, *Why Data Breaches Don't Hurt Stock Prices*, HARV. BUS. REV. (Mar. 31, 2015), https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices (arguing that even significant breaches have "very little impact" on the company's stock price).

42. Paul Bischoff, *Analysis: How Data Breaches Affect Stock Market Share Prices*, COMPARITECH (July 11, 2017), https://www.comparitech.com/blog/information-security/data-breach-share-price. In particular, the study focused on three concerns: (1) the immediate effect of a data breach on closing share price compared to daily volatility; (2) the percent difference in closing share price performance versus the S&P 500 over the same period of time from the day prior to a breach; and (3) the recovery time for that percent change to return to zero or greater. *Id.*

43. The study used NASDAQ's market performance as a baseline, rather than zero. *Id.* For example, if NASDAQ rose 2% and a company's stock rose 1%, the study would find a 1% decrease in that company's stock performance versus the market. If, however, NASDAQ fell 2% and a company's stock rose 2%, the study would find a 4% increase in that company's stock performance versus the market. *Id.*

44. The one-half percent drop was found to be within the standard deviation for daily volatility, rendering it statistically insignificant. *Id.* One year after the breach, the twenty-four companies' stocks underperformed NASDAQ by 7.33% on average. *Id.*

45. *Id.*

found negative long-term effects in the postbreach growth rate relative to the prebreach growth rate. While companies' share prices ultimately continued to increase following a data breach, postbreach growth, averaging 14.8%, was minute in comparison to prebreach growth, which averaged 45.6%.[46] While this study examined only significant data breaches,[47] it found that the smallest analyzed breaches—those with a lower number of records compromised—impacted share prices the most.[48] This demonstrates that a breach does not need to be of equal magnitude to the Equifax breach in order to harm shareholders. Ultimately, the described decrease in market value resulting from a content data breach damages shareholders.[49]

Additionally, data breaches result in both direct and indirect costs to the company, restricting its ability to grow in directions in which it otherwise would have been capable.[50] A data breach in the United States costs $7.35 million on average, which in turn, impacts a company's profitability.[51] For example, Equifax risks spending over $100 million dollars in costs,[52] in addition to

46. The study looked at share price growth in the three years prior to and three years after a data breach. *Id.*

47. In order to qualify for the study, the company must have: (1) been publicly listed, preferably on the New York Stock Exchange; (2) experienced a breach affecting one million or more records; and (3) publicly disclosed the breach. *Id.*

48. These breaches impacted 1–10 million company records and resulted in a 2% initial drop, 21-day recovery, and 5.91% subsequent drop 165 days after the breach. *Id.* The study also analyzed the companies' stock prices based on time of breach, the companies' industries, and sensitivity of stolen information. *Id.*; *see also* David Ruiz, *Data Breaches Have Lingering Effect on Stock Prices, Study Says*, LAW.COM: CORP. COUNS. (July 11, 2017), https://www.law.com/corpcounsel/sites/corpcounsel/2017/07/11/data-breaches-have-lingering-effect-on-stock-prices-study-says (discussing the Comparitech study and summarizing its results).

49. *See* Press Release, SEC, Statement on Cybersecurity (Sept. 20, 2017), https://www.sec.gov/news/press-release/2017-170 (stating that one of the risks associated with a data breach is "investor losses resulting from the theft of funds or market value declines in companies subject to cyberattacks").

50. *See* Michael Peters, *Post Equifax, New Data Breach Notification Laws Are Inevitable*, SECURITY BOULEVARD (Jan. 10, 2018), https://securityboulevard.com/2018/01/post-equifax-new-data-breach-notification-laws-are-inevitable (quoting SEC Chairman, Jay Clayton, stating that cyber breaches are "one of the greatest risks to the financial system right now"). *See generally* Emily Mossburg et al., *The Hidden Costs of an IP Breach*, 19 DELOITTE REV. 106, 118 (2016) (arguing that due to the "importance to growth market share, and innovation . . . cyber risk should rightly sit with other strategic initiatives managed at the C-suite level").

51. PONEMON STUDY, *supra* note 27, at 5, 10.

52. Mike Lennon, *Equifax: Hack Related Expenses Cost Company $87.5*

facing a multibillion-dollar lawsuit.[53] First, a data breach results in direct costs,[54] such as those related to engaging a forensic expert or cybersecurity firm to investigate the breach[55] and improving security measures moving forward.[56] For example, to thoroughly investigate and report its breach, Equifax incurred $17.1 million in professional fees.[57] Additionally, a company will often engage outside counsel to manage the expected litigation.[58] Finally, breached companies offer identity protection services and remedial options to its consumer base.[59] For example, Equifax announced three postbreach consumer protection offerings to mitigate consumer harm,[60] including credit monitoring,[61] freezing services,[62] and a "credit lock" tool.[63] These offerings will

Million in Q3, SECURITY WK. (Nov. 9, 2017), https://www.securityweek.com/equifax-hack-related-expenses-cost-company-875-million-q3.

53. *See* Polly Mosendz, *Equifax Faces Multibillion-Dollar Lawsuit over Hack*, BLOOMBERG (Sept. 8, 2017), https://www.bloomberg.com/news/articles/2017-09-08/equifax-sued-over-massive-hack-in-multibillion-dollar-lawsuit (describing a class action against Equifax by over 143 million consumers).

54. *See* PONEMON STUDY, *supra* note 27, at 29 (defining direct costs as "the direct expense outlay to accomplish a given activity").

55. *See* FED. TRADE COMM'N, DATA BREACH RESPONSE: A GUIDE FOR BUSINESS 1 (2016) [hereinafter FTC REPORT] (instructing companies to identify an independent data forensics team to help determine the source and scope of the breach, analyze the collected evidence, and advise on remediation steps).

56. *Contra* Erik Sherman, *The Reason Companies Don't Fix Cybersecurity*, CBS (Feb. 13, 2016), https://www.cbsnews.com/news/the-reason-companies-dont-fix-cybersecurity (suggesting the return is not worth large companies' investments in data protection measures, because the losses are small compared to the revenue of these corporate "behemoth[s]").

57. Lennon, *supra* note 52.

58. FTC REPORT, *supra* note 55, at 1 (instructing companies to consult with in-house attorneys before hiring outside counsel with privacy and data security expertise who may advise on applicable law and requirements). *But see* BRYAN CAVE, 2017 DATA BREACH LITIGATION REPORT 3 (2017) (finding that due to standing issues for the plaintiff, the risk that a company will face litigation following a data breach is relatively low).

59. *See, e.g.*, Lily Hay Newman, *Can Equifax's Offerings Actually Protect Your Identity?*, WIRED (Sept. 30, 2017), https://www.wired.com/story/equifax-identity-protection-offerings (quoting the founder of data security and privacy firm CyberScout, Adam Levin, as saying "[i]n the event something goes wrong, . . . companies need to respond urgently, transparently, and empathetically").

60. *See id.* (describing and discussing Equifax's response measures).

61. A credit-monitoring service sends an individual an alert so he or she may catch suspicious activity earlier than later. *Id.*

62. A freezing service locks down an individual's credit files that requires new entities to get specific permission and pin numbers from the individual before accessing his or her information for the first time. *Id.*

63. A "credit lock" tool allows consumers to lock and unlock access to their data at any time. *Id.*

cost Equifax approximately $14.9 million.[64] Nonetheless, breached companies often institute these services and options in the hopes of increasing consumer retention and its general public perception.[65]

Customer retention and public perception themselves are among the indirect costs[66] of a data breach.[67] A breach can greatly harm consumer and shareholder trust, which culminates in decreased customer attainment and retention, and ultimately a devaluation of the brand itself.[68] Recent studies have found that the average loss to brand value following a data breach ranged from $184 to $332 million.[69] A further indirect cost is lost business,[70] a term which encompasses not only "reputation losses and diminished goodwill," but also broader costs.[71] These broader costs include increased difficulty in attracting new customers[72] and loss of intellectual property and trade secrets.[73] When a company loses its intellectual property and trade secrets, its competitive edge is compromised.[74] The company may

64. Lennon, *supra* note 52.

65. *See Why Companies Should Offer Post-Breach Monitoring Services*, EXPERIAN (Aug. 4, 2017), http://www.experian.com/blogs/data-breach/2017/08/04/companies-offer-post-breach-monitoring-services (finding that companies who successfully help consumers results in better retention and prevents losing consumers to the competition).

66. *See* PONEMON STUDY, *supra* note 27, at 29 (defining indirect costs as "the amount of time, effort[,] and other organizational resources allocated to data breach resolution, but not as a direct cash outlay").

67. *See id.* at 22 (measuring "reputation losses and diminished goodwill").

68. *See The Consequences of a Cyber Security Breach*, SUNGARD AVAILABILITY SERVICES., https://www.sungardas.com/en/cyber-security-advice/articles/the-consequences-of-a-cyber-security-breach.html (last visited Mar. 10, 2019).

69. PONEMON INST., 2011 REPUTATION IMPACT OF A DATA BREACH 1 (2011). *But see* Sherman, *supra* note 56 (stating that "[n]ew customer acquisition can be a problem, but probably not a permanent one," and claiming that the public's perception is back to normal within six months of a breach).

70. *See* PONEMON STUDY, *supra* note 27, at 22 (finding that the average lost business cost over a period of twelve years was $4.13 million).

71. PONEMON INST., 2011, *supra* note 69.

72. *See 86% of Customers Would Shun Brands Following a Data Breach*, SEMAFONE (Mar. 2014), https://semafone.com/press-releases/86-customers-shun-brands-following-data-breach (finding that eighty-six percent of survey participants either were very unlikely to or would not do business with a company that had previously experienced a data breach involving financial information).

73. Mossburg et al., *supra* note 50, at 108.

74. *Id.* (suggesting that while there are fewer upfront, direct costs, "losing IP could mean forfeiture of first-to-market advantage, loss of profitability, or—in the worst case—losing entire lines of business to competitors or counterfeiters").

not realize the extent of the resulting competitive disadvantage until much later, after observing that several "strategies fail to yield positive results."[75] This risk is particularly pronounced when a company, such as Equifax, does not discover the breach for an extended period of time.[76]

These types of damages and harms that result from data breaches are of the type that prompted Congress to create a federal disclosure regime and a governing agency to ensure compliance. The remainder of this Part details this regime.

B. PURPOSE AND PROCEDURES OF THE 1933 AND 1934 SECURITIES ACT

Each shareholder holds a right to future cash flow of the corporation.[77] This right, in turn, creates an interest in the company. Until 1933, effective market regulation was nonexistent and market information was rarely available to the individual investor as a result.[78] Individuals nonetheless continued investing until the unprecedented market crash in 1929.[79] In 1933, President Franklin Roosevelt urged Congress to adopt measures to regulate the national securities market, a move which would be "but one step in [its] broad purpose of protecting investors."[80] The Securities Act of 1933 (Securities Act) and the Securities Exchange Act of 1934 (Exchange Act) reflected this desire to protect investors and to promote efficiency.[81] The Securities Act requires

75. *3 Long Term-Data Breach Consequences*, GLOBALSCAPE (Nov. 11, 2013), https://www.globalscape.com/blog/2013/11/11/3-long-termdata-breach-consequences.

76. *See supra* notes 9, 11, and accompanying text (stating that Equifax first discovered the data breach on July 29, 2017, though the hackers first began accessing information on May 13, 2017).

77. *See, e.g.*, Michael J. Mauboussin, *What Shareholder Value Is Really About*, HARV. BUS. REV. (Oct. 3, 2011), https://hbr.org/2011/10/ceos-must-understand-what-crea (stating that investors essentially make "short-term bets on long-term outcomes," while explaining that the "value of the business is the present value of future cash flows").

78. *See* Giulio Pontecorvo, *Investment Banking and Security Speculation in the Late 1920's*, 32 BUS. HIST. REV. 166, 168 (1958) (stating that the "American capital market in the 1920's was still independent of any significant constraints on freedom of action" both from governmental entities and large institutional investors); *see also What We Do*, SEC, https://www.sec.gov/Article/whatwedo.html (last updated June 10, 2013) (explaining that prior to 1929, there was "little support for federal regulation of the securities markets").

79. *See* Gene Smiley, *US Economy in the 1920s*, EH.NET ENCYCLOPEDIA (2004), https://eh.net/encyclopedia/the-u-s-economy-in-the-1920s.

80. *See* H.R. REP. NO. 73-1383, at 2 (1934).

81. *See* Securities Exchange Act, 15 U.S.C. § 78c(f) (2012); *see also* H.R.

companies to register publicly-offered securities, which Congress hoped would enable investors to make more informed business judgments.[82] The Exchange Act established the SEC[83] and granted it power to provide for periodic reporting requirements in order to supplement an investor's ability to form a well-reasoned judgment of the value of securities he or she buys and sells.[84] This legislation granted the SEC broad authority, allowing the agency to promulgate rules and regulations to achieve the Exchange Act's purpose: protecting investors and enhancing transparency to allow for informed investments.[85]

The SEC has used its broad discretion to create an elaborate scheme of disclosure requirements, which apply to most U.S. public companies. For example, the SEC mandates that publicly traded companies file quarterly reports, or 10-Qs, which include information regarding stock repurchases, inventory turnover, changes in working capital, and potential legal risks, such as lawsuits.[86] SEC rules and regulations have evolved throughout over time in response to the purpose of the Exchange Act, shifting investor interests, and external events that make certain information more relevant to a company's shareholders. This approach is consistent with Congress's original intent to create a

REP. NO. 73-1383, at 2 (explaining that the Act was intended to rectify the dangerous speculation of securities that characterized the 1920s). The Committee on Interstate and Foreign Commerce attributed this "excessive" speculation primarily to "inadequate corporate reporting," which resulted in investor ignorance of critical factors necessary for "intelligent judgment of the values of securities." *Id.* at 4–5.

82. *See The Laws That Govern the Securities Industry*, SEC, https://www.sec.gov/answers/about-lawsshtml.html (last visited Mar. 10, 2019). This mandatory registration form requires companies to disclose: (1) a description of the company's properties and business; (2) a description of the security to be offered for sale; (3) information about the management of the company; and (4) financial statements certified by independent accountants. *Id.*; *see also* 15 U.S.C. § 77g (establishing requirements for SEC registration).

83. *See* 15 U.S.C. § 77g.

84. *See* H.R. REP. NO. 73-1383, at 6.

85. *See id.* at 6–7 (recognizing that an administrative agency is best suited to adopt regulations in a field such as securities where "practices constantly vary").

86. *See* Joshua Kennon, *Annual Reports, 10-Ks, and 10-Qs*, THE BALANCE (June 29, 2017), https://www.thebalance.com/annual-reports-10k-10q-357266. This form provides investors with information that "give[s] insight into changes that are happening in a business long before those changes show up in the earnings figures." *Id.*

stable and efficient market, which will, in turn, attract further investment to fuel growth.[87]

C. AMENDMENTS TO AND EXPANSIONS OF THE 1933 AND 1934 ACT

Shareholder interests are an influential factor in SEC rulemaking. In some instances, lack of shareholder interest has been influential in the SEC's decision not to impose additional disclosure requirements. For example, in 1975, the SEC concluded that disclosure related to social-policy interests was not necessary.[88] In so deciding, the agency noted that corporations had not received a significant number of social inquiries from their shareholders, and further, that the few shareholder proposals relating to social policy had received extremely low shareholder support.[89] In other instances, shareholder interest has prompted the SEC to impose additional requirements. In the wake of the 2008 financial crisis, the SEC amended its rules in 2009, providing investors with greater insight as to how managers of corporations oversee risk taking.[90] The agency promulgated the amendments in response to investors' increased focus on corporate accountability and "desire for additional information that would enhance their ability to make informed voting and investment decisions."[91]

87. *See* Eric D. Roiter, *Illegal Corporate Practices and the Disclosure Requirements of the Federal Securities Laws*, 50 FORDHAM L. REV. 781, 784–85 (1982) (summarizing the "subsidiary" purposes of the Exchange Act as (1) improved pricing mechanisms resulting from informed investor assessments; (2) enhanced investor confidence, leading to increased stability and greater infusions of capital for industry and commerce; and (3) deterrence of corporate misconduct); *see also* H.R. REP. NO. 73-1383, at 11 ("The idea of a free and open public market is built upon the theory that competing judgments of buyers and sellers as to the fair price of a security brings about a situation where the market price reflects as nearly as possible a just price.").

88. *See* Environmental and Social Disclosure, 40 Fed. Reg. 51,656, 51,656 (proposed Nov. 6, 1975) (codified at 17 C.F.R. pts. 239, 240, 249); *cf.* Barnali Choudhury, *Social Disclosure*, 13 BERKELEY BUS. L.J. 183, 195–98 (2016) (discussing whether social disclosure requirements—disclosures that are related to social issues—help or harm shareholder interests in today's marketplace).

89. Environmental and Social Disclosure, 40 Fed. Reg. at 51,664 (noting a two to three percent voting approval on these issues in recent years).

90. *See* Proxy Disclosure Enhancements, 74 Fed. Reg. 68,334, 68,334 (Dec. 23, 2009) (codified at 17 C.F.R. pts. 229, 239, 240, 249, 274).

91. *Id.* The SEC stated that investors supported "the manner in which [the SEC] proposed to achieve these objectives," and ultimately adopted the amendments, despite opposition from "other commentators." *Id.* at 68,335.

Additionally, the SEC has adopted rules in response to external events or societal changes that render particular information more important to shareholders. The SEC's 2009 amendments, promulgated in response to external events such as the 2008 financial crisis[92] and the passing of the Sarbanes-Oxley Act in 2002, demonstrate this flexibility.[93] The Sarbanes-Oxley Act, itself, added new and expanded existing disclosure requirements that would provide greater investor protection.[94] The enactment of this Act was largely due to Enron's unexpected filing for bankruptcy, demonstrating Congress's desire to regulate in response to events affecting the economy[95]—such as content data breaches—thus, endorsing the SEC's choice to do the same. Additionally, the Sarbanes-Oxley Act further expanded the SEC's resources and authority to effectively regulate in the face of the securities market's "unprecedented growth and change."[96]

D. FORM 8-K AND ITS 2004 EXPANSION

In 2004, the SEC invoked its authority to widen the scope of Form 8-K, a form used to notify investors of specified events on a periodic basis.[97] Form 8-K allows companies to release infor-

92. *See* Proxy Disclosure and Solicitation Enhancements, 74 Fed. Reg. 35,076, 35,080 (July 17, 2009) (codified at 17 C.F.R. pts. 229, 239, 240, 249, 270, 274) (explaining that volatility in stock price, "such as the significant decreases during 2008" affect total compensation, thus demonstrating that disclosure requirements relating to compensation policies are necessary).

93. *Id.* at 35,083 (explaining that "developments, such as the enactment of the Sarbanes-Oxley Act of 2002 and corporate-governance related listing standards . . . have brought about significant changes in the structure and composition of corporate boards" thus demonstrating that disclosure requirements related to director qualifications are necessary).

94. *See* Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (codified in scattered sections of 15, 18, and 28 U.S.C.).

95. *See* S. REP. NO. 107-205, at 29 (2002) ("This Committee recognizes from the recent experience of Enron Corp. and other public companies the need for additional types of disclosures."). The Report references testimony of the former SEC Chairman, Richard Breeden, following the Enron scandal, in which he urges additional disclosure requirements for "off-balance sheet transactions and debt." *Id.* at 28 (internal citations and quotation marks omitted).

96. *Id.* at 40.

97. FORM 8-K, *supra* note 35; *see also* Additional Form 8-K Disclosure Requirements and Acceleration of Filing Date, 67 Fed. Reg. 42,914, 42,914 (June 25, 2002) [hereinafter Proposed 2002 Rule] (providing that the SEC created Form 8-K in 1936, "as the form to be used by companies to file 'current' reports when specific extraordinary corporate events occur" (citing Release No. 34-925 (Nov. 11, 1936))).

mation that the Exchange Act, and other rules promulgated pursuant to this Act, require companies to disclose.[98] For example, Regulation Fair Disclosures (FD) requires companies to make market-sensitive information available to all parties—including institutional investors, individual investors, and the general public—at the same time.[99] A company may fulfill this requirement with an 8-K filing containing such market-sensitive information.[100]

The 2004 Final Rule (the 2004 Rule) expanded the number of reportable events on Form 8-K.[101] Specifically, the 2004 Rule added eight new items to the form, transferred two items from the periodic reports, and expanded disclosures under two items on the former Form 8-K.[102] Additionally, the 2004 Rule reorganized the disclosure items into topical categories and shortened the filing deadline to four business days after the occurrence of a triggering event.[103] Ultimately, these changes increased Form 8-K's power to facilitate timely communication between a company and its shareholders, as well as the public. Indeed, the amendments were a response to the 'real time issuer disclosure' mandate in Section 409 of the Sarbanes-Oxley Act of 2002,[104] and are intended to benefit investors.[105] The SEC explained:

98. FORM 8-K, *supra* note 35.

99. *See* Selective Disclosure and Insider Trading, 65 Fed. Reg. 51,716, 51,718 (Aug. 24, 2000) (codified at 17 C.F.R. pts. 240, 243, 249).

100. FORM 8-K, *supra* note 35, at 2 (stating that Form 8-K "shall be used for . . . reports of nonpublic information required to be disclosed by Regulation FD" and that the form "satisfies all the substantive requirements" of the FD regulation).

101. *See* Additional Form 8-K Disclosure Requirements and Acceleration of Filing Date, 69 Fed. Reg. 15,594, 15,594 (Mar. 25, 2004) (codified at 17 C.F.R. pts. 228, 229, 230, 239, 240, 249) [hereinafter 2004 Rule]; *see also* Proposed 2002 Rule, *supra* note 97, at 42,914 (stating the then-current Form 8-K requirements as including nine disclosure items and a five-day filing deadline). *See generally* 17 C.F.R. § 249.308 (2018) (providing that Form 8-K will be used for "current reports").

102. 2004 Rule, *supra* note 101, at 15,596.

103. *See id.*; *cf.* Proposed 2002 Rule, *supra* note 97, at 42,914 (stating that the former filing deadline was five days). The 2004 Rule additionally adopts a limited "safe harbor" provision from liability for failure to timely file a Form 8-K for certain items. 2004 Rule, *supra* note 101, at 15,606.

104. Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, § 409, 116 Stat. 745 (codified in scattered sections of 15, 18, and 28 U.S.C.) (requiring "rapid and current" disclosure of such information as the SEC determines necessary "for the protection of investors").

105. *See* 2004 Rule, *supra* note 101.

> Under the previous Form 8-K regime, companies were required to report very few significant corporate events. The limited number of Form 8-K disclosure items permitted a public company to delay disclosure of many significant events until the due date for its next periodic report. During such a delay, the market was unable to assimilate such undisclosed information into the value of a company's securities. The revisions that we adopt today will benefit markets by increasing the number of unquestionably or presumptively material events that must be disclosed currently. They will also provide investors with better and more timely disclosure of important corporate events.[106]

Thus, the SEC hoped that the 2004 Rule would promote transparency by increasing the frequency and volume of corporate reporting. The current Form 8-K now lists nine Sections containing a total of twenty-two Items that companies must disclose within four days to their investors and the public.[107] Most relevant for the purposes of this Note is Item 2.06: Material Impairments, listed under the Financial Information heading of Section Two.[108] A company triggers this disclosure requirement when it "concludes that a material charge for impairment to one or more of its assets, including, without limitation, an impairment of securities or goodwill, is required under generally accepted accounting principles applicable to the company."[109] The broad coverage of this catch-all item[110] reflects the SEC's intent to encourage corporate transparency in order to protect investors.[111]

E. MATERIALITY AS THE TOUCHSTONE OF FEDERAL SECURITIES LAW

Materiality is a familiar concept in securities law, continuously appearing in statutes, regulations, and judicial opinions.

106. *Id.* at 15,594–95.

107. *Id.*

108. *Id.* at 15,601.

109. *Id.* The company must disclose information including: (1) "impaired asset or assets and the facts and circumstances leading to the conclusion that the charge for impairment is required;" (2) "the company's estimate of the amount or range of amounts of the impairment charge;" and (3) "the company's estimate of the amount or range of amounts of the impairment charge that will result in future cash expenditures." *Id.*

110. *See infra* notes 115–17 and accompanying text.

111. *See* Proposed 2002 Rule, *supra* note 97, at 42,915 (discussing the expansion of 8-K requirements and imposition of deadlines throughout history in order to provide investors with "timely, high-quality" information, and noting this Rule as the latest such expansion).

Congress incorporated the materiality standard first into the Securities Act,[112] and then again one year later, in the Exchange Act.[113] Throughout its course of developing a disclosure framework, the SEC has similarly infused the materiality standard into rules and regulations.[114] Often, the SEC dedicates hundreds of pages to detailed disclosure requirements, followed by a catch-all obligation to disclose "all other material information."[115] Item 2.06: Material Impairments on Form 8-K is one such catch-all.[116] Thus, for more than eighty years, materiality has been the touchstone of securities law, governing the way in which companies must disclose information to the public and investors.[117] This Section will provide the most commonly used definition of materiality and the justifications for this definition's widespread adoption.

1. Defining the Standard

In 1973, the U.S. Supreme Court decided *TSC Industries, Inc. v. Northway, Inc.* and articulated the definition of materiality that is most commonly accepted today:

> An omitted fact is material if there is a substantial likelihood that a reasonable shareholder *would* consider it important in deciding how to vote . . . . Put another way, there must be a substantial likelihood that the disclosure of the omitted fact would have been viewed by the rea-

112. Securities Act § 17(a), 15 U.S.C. § 771q (2012) (declaring it unlawful to "obtain money or property by means of any untrue statement of a material fact or any omission to state a material fact").

113. Securities Exchange Act § 18(a), 15 U.S.C. § 78r (imposing liability on any person "who shall make or cause to be made any false and misleading statement of material fact in any application, report, or document filed under the act").

114. *See, e.g.*, 17 C.F.R. § 240.10b–5 (2018) (governing the selling and purchasing of securities); *id.* § 243.100 (governing simultaneous disclosure to investment institutions, individual investors, and the public).

115. *See, e.g.*, *id.* § 240.12b–20 (governing reports, forms and schedules filed under the Exchange Act); 18 C.F.R. § 385.408 (2018) (governing forms filed under the Securities Act).

116. FORM 8-K, *supra* note 35, at 2.

117. *See* BUS. ROUNDTABLE, THE MATERIALITY STANDARD FOR PUBLIC COMPANY DISCLOSURE: MAINTAIN WHAT WORKS 3 (2015) [hereinafter BUSINESS ROUNDTABLE] (arguing that the concept of materiality has been the "cornerstone" of securities laws since Congress first embedded it in the Securities Act). The Business Roundtable is an association of chief executive officers collectively leading companies with more than seven trillion dollars in annual revenues and more than sixteen million employees. *Id.* at 1.

> sonable investor as having significantly altered the 'total mix' of information made available.[118]

The Court reaffirmed this standard in *Basic v. Levinson*, emphasizing that the determination of whether a piece of information is material is an "inherently fact-specific finding."[119]

Subsequently, the SEC and companies subject to SEC regulations have adopted the *TSC Industries* standard. For example, in 1982, the SEC amended Rule 405 under the Exchange Act and expressly adopted the "reasonable investor" materiality standard.[120] Companies rely on this definition when preparing annual and periodic reports under SEC regulations.[121] Courts across the nation have used this standard when determining liability in securities suits.[122] This widespread adoption may support relying on the "reasonable investor" standard when determining materiality in the future.

2. The Reason for the Materiality Standard's Prominence

The "reasonable investor" standard focuses attention directly on the issue Congress identified in its enactment of the

118. 426 U.S. 438, 449 (1976) (emphasis added) (citations omitted). *TSC Industries* followed the Court's previous attempt to define materiality in *Mills v. Electric Auto-Lite Co.*, 396 U.S. 375 (1970). In *Mills*, the Court defined material information as information "of such a character that it might have been considered important by a reasonable shareholder" in the voting process. *Id.* at 384. The Court stated that this definition most closely comports with the SEC's policies in protecting investors and is "fully consistent with *Mills*." *TSC Indus.*, 426 U.S. at 449. Some scholars have argued that by leaving *Mills* intact, the earlier decision cabined and constrained the latter's opportunity to define the critical term. *See, e.g.*, Dale A. Oesterle, *The Overused and Under-Defined Notion of "Material" in Securities Law*, 14 U. PA. J. BUS. L. 167, 175–76 (2011) (arguing that Court should have overruled *Mills* and "started from scratch").

119. 485 U.S. 224, 236 (1988) (finding "no valid justification" for excluding pre-merger talks and insider trading from the *TSC Industries* definition of materiality). Proxy fraud and insider trading are prohibited by Section 10(b) of the Exchange Act and the SEC's Rule 10b–5, respectively. Securities Exchange Act § 10(b), 15 U.S.C. § 78j (2012); 17 C.F.R. § 240.10b–5 (2018).

120. 17 C.F.R. §§ 230.405, 240.12b–20 (defining materiality as "those matters to which there is a substantial likelihood that a reasonable investor would attach importance in determining whether to purchase the security registered").

121. *See, e.g.*, BUS. ROUNDTABLE, *supra* note 117, at 3 (describing the SEC's history of defining materiality).

122. *See, e.g.*, Dalberth v. Xerox Corp., 766 F.3d 172, 183 (2d Cir. 2014) ("To fulfill the materiality requirement, 'there must be a substantial likelihood that the disclosure of the omitted fact would have been viewed by the reasonable investor as having significantly altered the total mix of information available.'" (quoting Basic, Inc. v. Levinson, 485 U.S. 224, 231–32 (1988))); Petrie v. Elec. Game Card, Inc., 761 F.3d 959, 970 (9th Cir. 2014) (same).

Acts of 1933 and 1934.[123] Congress established both these Acts and the SEC to protect investors and to eliminate unnecessary speculation from the securities market.[124] Writing for the Court in *TSC Industries*, Justice Marshall directly acknowledged that the "reasonable investor" standard must achieve this purpose.[125] Before articulating the standard, Justice Marshall clarified that the court was not just guided by an intent to reach a judicially fair and equitable outcome, but more importantly, to "ensure disclosures by corporate management in order to enable the shareholders to make an informed choice."[126]

Moreover, the "reasonable investor" standard strikes the balance that the notion of materiality strives to achieve.[127] In *TSC Industries*, Justice Marshall recognized the danger in a materiality bar that is too low by noting that some information is so "dubious" that disclosure of such would result only in investor confusion and excessive corporate compliance costs.[128] Thus, in order to avoid liability under a broad definition of materiality, companies would be tempted to "bury the shareholders in an avalanche of trivial information[,] a result that is hardly conducive to informed decisionmaking."[129] Furthermore, issues and concerns become more and less important to shareholders as societal circumstances change. Framing the standard in the perspective of a reasonable investor allows the standard to evolve with developments in the broader economy.[130]

While the "reasonable investor" is widely adopted and achieves several objectives in securities law, it is not without flaws. The standard often looks backward, assessing materiality after the fact in a court proceeding with the benefit of additional

123. *See supra* notes 81–85 and accompanying text (detailing the history and background of the Securities Act and Exchange Act).

124. *See* H.R. REP. NO. 73–1383, at 1–2 (1934) (capturing President Roosevelt's recommendation to Congress to enact legislation—the Exchange Act—to provide regulation in order to protect investors).

125. TSC Indus., Inc. v. Northway, Inc., 426 U.S. 438, 449 n.10 (1976) ("In defining materiality . . . we are, of course, giving content to a rule promulgated by the SEC pursuant to broad statutory authority to promote 'the public interest' and 'the protection of investors.'" (citations omitted)).

126. *Id.* at 448.

127. *See infra* notes 160–64 and accompanying text (discussing the balance that the materiality standard strikes).

128. *TSC Indus.*, 426 U.S. at 448.

129. *Id.* at 448–49.

130. *See* BUS. ROUNDTABLE, *supra* note 117, at 8 (explaining that the standard provides a "framework for addressing new issues and shedding issues whose importance has waned").

facts, empirical evidence, market reactions, and actual significance to shareholders.[131] As there is little guidance beyond the standard itself, firms and courts may develop their own rules of thumb to use as thresholds when assessing materiality.[132] While discouraged by the SEC,[133] numeric thresholds are difficult to resist in assessing an ambiguous standard.[134] Additionally, this standard provides large firms with more leeway in interpreting materiality than it does for small firms.[135] A larger firm entails a larger and more complex "total mix of information,"[136] in turn, raising the threshold at which information will become material.[137] This higher threshold then allows larger firms to interpret materiality and to avoid disclosing events with a flexibility

131. *See* Mitu Gulati et al., *Fraud by Hindsight*, 98 NW. U. L. REV. 773, 788 (2004) (explaining that when presented with the occurrence of a bad event, a judge is more likely to determine that a prior event rendered disclosure necessary based on the present knowledge that the event occurred). *See generally id.* at 788–91 (discussing hindsight bias as it relates to determinations of materiality). Recent SEC regulations urge entities to focus on expected market reactions to information, leaving the courts to use price impact as a proxy for materiality. *See* Michael J. Kaufman & John M. Wunderlich, *Regressing: The Troubling Dispositive Role of Event Studies in Securities Fraud Litigation*, 15 STAN. J.L. BUS. & FIN. 183, 199–201 (2009) (collecting cases that demonstrate that materiality assessments depend on a showing of post-disclosure price movement).

132. *See* SEC Staff Accounting Bulletin No. 99, 64 Fed. Reg. 45,150, 45,152 (1999), https://www.sec.gov/interps/account/sab99.htm (stating that many companies and auditors use a five percent threshold as a rule of thumb in assessing materiality); *see also* Parnes v. Gateway 2000, 122 F.3d 539, 547 (8th Cir. 1997) (holding that the defendant's alleged overstatement of assets by $6.8 million—amounting to two percent of the fast-growing company's total assets—was not material because a reasonable investor "would not have been put off by an asset column that was 2% smaller").

133. *See* SEC Staff Accounting Bulletin No. 99, 64 Fed. Reg. at 45,151 (stating that numerical thresholds may only be used as an "initial step in assessing materiality" and further, that materiality cannot be reduced to a quantitative formula). The SEC Staff elaborates, explaining that the totality of circumstances must be accounted for, including both quantitative and qualitative considerations. *Id.*

134. *See, e.g.*, Sarah Johnson, *SEC, PCAOB Pushed to Define Materiality*, CFO (June 20, 2007), http://ww2.cfo.com/accounting-tax/2007/06/sec-pcaob-pushed-to-define-materiality (discussing auditors' desires for the SEC to establish quantitative measures for materiality).

135. *See generally* George S. Georgiev, *Too Big to Disclose: Firm Size and Materiality Blindspots in Securities Regulation*, 64 UCLA L. REV. 602, 625–42 (2017) (demonstrating, in the context of certain disclosure areas, how materiality provides larger firms with greater flexibility in assessing materiality).

136. TSC Indus., Inc. v. Northway, Inc., 426 U.S. 438, 449 (1976).

137. *See* Georgiev, *supra* note 135, at 625 ("The size and complexity of large firms gives them a much larger 'total mix,' which—in turn—sets a very high threshold for what should . . . be disclosed.").

unavailable to smaller firms.[138] Despite these flaws, however, materiality and the *TSC Industries* standard remain prominent in the realm of corporate disclosure law.

The SEC embodies materiality as a guidepost for regulating in response to shareholder interests and changing externalities, and ultimately, in fulfilling the purposes of disclosure law. The agency's mandate from Congress to adopt regulations in the face of market changes in combination with its administrative flexibility allows the SEC to explicitly impose disclosure regulations relating to content data breaches. The remainder of this Note argues that the SEC should take such action via a rule, rather than a standard.

II. A RULE—RATHER THAN A STANDARD—OF MATERIALITY

Part I of this Note discussed the SEC's authority to mandate corporate disclosures, the purposes the SEC aims to promote through such mandates, and the standard it often uses to trigger disclosure. Part II challenges the use of a standard, arguing instead for a bright line rule which will provide clarity by requiring that companies disclose content data breaches. This Part first briefly discusses the distinction between a standard and a rule before examining contexts in which the SEC has elected to use a rule, as opposed to its familiar standard, to establish an event's materiality. Finally, this Part concludes that a rule is better suited to establish a content data breach's materiality.

A. RULE OR STANDARD: THE DISTINCTION

The decision—and its accompanying tradeoffs—between a rule and a standard is a familiar topic in legal literature.[139] The difference between the two is in large part a degree of specificity.

138. *See id.* at 609 (explaining that this size discrepancy may result in an unfair competitive advantage to larger firms, who, for example, may be able to acquire a small company for an "immaterial" value, therefore avoiding disclosure and gaining advantage over a smaller firm, who, by doing the same, would be required to disclose such acquisition).

139. *See generally, e.g.*, Michael Coenen, *Rules Against Rulification*, 124 YALE L.J. 644 (2014); Louis Kaplow, *Rules Versus Standards: An Economic Analysis*, 42 DUKE L.J. 557 (1992); Duncan Kennedy, *Form and Substance in Private Law Adjudication*, 89 HARV. L. REV. 1685 (1976); Pierre Schlag, *Rules and Standards*, 33 UCLA L. REV. 379 (1985); Kathleen M. Sullivan, *The Supreme Court, 1991 Term—Foreword: The Justices of Rules and Standards*, 106 HARV. L. REV. 22 (1992); Cass R. Sunstein, *Problems with Rules*, 83 CALIF. L. REV. 953 (1995).

Rules are bright-line: they provide explicit guidance, leaving little room for future improvisation.[140] Standards, on the other hand, are flexible: they require particular application, ebbing and flowing with differing sets of facts and circumstances.[141]

Rules embody specificity. When Congress, the Supreme Court, or an administrative agency enacts a rule, they create uniformity, enhance predictability, and decrease the cost of decision making.[142] To that end, rules prevent "official arbitrariness."[143] A rule can either prohibit or require conduct—such as requiring disclosure of content data breaches. This bright-line clarity prevents entities, such as judges, from arbitrarily finding the regulated actors either complied with or violated the rule in any given circumstance.[144] Relatedly, if regulated parties know with certainty what conduct is prohibited or required, and therefore, what conduct violates the rule, they are better able and more likely to conform their conduct to the rule's prescription.[145] Additionally, this decreases compliance costs, often incurred in the form of legal fees.[146]

Rules, however, lack flexibility. For example, when the SEC issues a rule rather than a standard, it prohibits itself from developing and shaping that rule with time.[147] This sacrifices the ability to apply case-specific precision in order to best promote the goals and purposes underlying the rule.[148] Such a lack of precision often leads to over- and under-inclusion.[149] Additionally, a rule is costly to enact, requiring a much greater investment in

140. *See* Sullivan, *supra* note 139, at 58 (stating that a "legal directive is 'rule'-like when it binds a decisionmaker to respond in a determinate way to the presence of delimited triggering facts").

141. *See id.* (stating that a "legal directive is 'standard'-like when it tends to collapse decisionmaking back into the direct application of the background principle or policy to a fact situation").

142. *See* Coenen, *supra* note 139, at 652 (noting that a rule "falls toward the high end of the specificity spectrum").

143. *See* Kennedy, *supra* note 139, at 1688 ("[R]ules . . . are the restraint of official arbitrariness . . . .").

144. *Id.*

145. *Id.* at 1688–89 ("[I]f private actors can know in advance the incidence of official intervention, they will adjust their activities in advance to take account of them.").

146. *See* Kaplow, *supra* note 139, at 571–72 (discussing the cost of legal advice under rules versus standards).

147. *See* Coenen, *supra* note 139, at 646 (explaining that standards permit "nuance, flexibility, and case-specific deliberation").

148. *See* Kennedy, *supra* note 139, at 1689 (noting that rules lack case-specific deliberation).

149. *Id.*

resources to determine the appropriate threshold at which to impose liability.[150] These drawbacks simultaneously function as the benefits of a standard.

When Congress, the Supreme Court, or an administrative agency sets forth a standard, they allow space for future considerations and the ability to decide issues on a case-by-case basis.[151] Common examples of standards are reasonableness, due care, fairness, good faith, and—most importantly for this Note's purposes—materiality.[152] The generality of a standard allows its initial enactment to remain broad, covering wide subject matter and leaving gaps for future adjudications to fill with nuanced guidance.[153] In this endeavor, a judge will assess particular facts in terms of the purposes or social values underlying the standard, striving to avoid over- and under-inclusion.[154] This approach is particularly effective when "the range of relevant variables is very wide and [] rigidly rule-bound decisions could produce much error and injustice."[155] Standards, however, entail high compliance costs, uncertainty, and unpredictability—each of which, a rule counters.[156] Nonetheless, due to the broad factors relevant to the securities market, the SEC has often opted to issue standards, rather than rules, in its regulatory efforts.

B. RULE OR STANDARD: WHEN AND WHERE FOR THE SEC

The SEC has embedded a materiality *standard* into much of its regulatory framework.[157] Like most standards, materiality is often a facts and circumstances analysis.[158] Through this approach, the SEC strives to strike a balance between over- and

150. *See* Kaplow, *supra* note 139, at 577–78 (explaining that "[r]ules cost more to promulgate" than standards).

151. *See* Coenen, *supra* note 139, at 646 (explaining that standards permit "nuance, flexibility, and case-specific deliberation").

152. Kennedy, *supra* note 139, at 1688.

153. *See id.* at 1689 (describing the purpose of a general standard).

154. *Id.*

155. Sunstein, *supra* note 139, at 993.

156. Coenen, *supra* note 139, at 649 (elaborating on the pros and cons of rules and standards).

157. *See supra* notes 113–17 and accompanying text (describing the "reasonable investor" standard).

158. TSC Indus., Inc. v. Northway, Inc., 426 U.S. 438, 450 (1976) (declaring that materiality involves "the application of a legal standard to a particular set of facts"); *see also* Basic v. Levinson, 485 U.S. 224, 236 (1988) (noting that materiality turns on the facts (quoting *TSC Indus.*, 426 U.S. at 450)); Justin Indus., Inc. v. Choctaw Sec., 920 F.2d 262, 267 (5th Cir. 1990) ("In general, materiality is a question reserved to the fact-finder."); Sioux, Ltd., Sec. Litig. v. Coopers &

under-disclosure by limiting disclosure to relevant information.[159] This avoids excessively burdening companies, which practically cannot be expected to disclose every bit of known information.[160] More importantly, this balance also ensures that investors are not overwhelmed with a surplus of irrelevant information.[161] Additionally, the materiality standard is flexible, allowing the SEC and the judicial system to adapt to changing societal and economic concerns.[162] It further allows companies to tailor the standard to their relevant industry and circumstances.[163] This flexibility is critical for the SEC to effectively regulate the securities market, which is a dynamic and evolving space.[164] These justifications underlie the standard present in several SEC regulations, including the 2004 Rule.[165]

However, the SEC has declared particular events and categories of information as exceptions to this materiality standard, instead providing for a rule in these contexts of corporate disclosures. The rules provide clarity in these particular contexts by

Lybrand, 914 F.2d 61, 65–66 (5th Cir. 1990) (same) (quoting *TSC Indus.*, 426 U.S. at 450); Michaels v. Michaels, 767 F.2d 1185, 1196 (7th Cir. 1985) (explaining the test for materiality is an objective one (citing *TSC Indus.*, 426 U.S. at 445)); Thomas v. Duralite Co., 524 F.2d 577, 581, 584–85 (3d Cir. 1975) (noting that materiality turns on the facts); Kohler v. Kohler Co., 319 F.2d 634, 642 (7th Cir. 1963) (analyzing specific facts to determine materiality).

159. *See* Kennedy, *supra* note 139, at 1689 (discussing the need for balanced rules).

160. *See* Nat. Res. Def. Council, Inc. v. SEC, 606 F.2d 1031, 1041 (D.C. Cir. 1979) (articulating the SEC's argument that required disclosure of immaterial information would burden companies with unmanageable disclosure expectations and would "significantly increase the costs to all involved without . . . corresponding benefits to investors generally").

161. *See* Mary Jo White, Chair, SEC, A.A. Sommer, Jr. Corporate Securities and Financial Law Lecture: The Importance of Independence (Oct. 3, 2013), https://www.sec.gov/news/speech/spch100113mjw#.VEasLvnF98E ("When disclosure gets to be too much or strays from its core purposes, it can lead to 'information overload' . . . mak[ing] it difficult for investors to focus on information that is material and most relevant to their decision-making as investors in our financial markets.").

162. *See* BUS. ROUNDTABLE, *supra* note 117, at 6–7, 14 (explaining that the definition of materiality may evolve overtime, and therefore, that when a societal concern becomes material, "disclosure of that information is already required").

163. *Id.* at 6 (stating that the flexibility of the materiality standard allows its definition to vary according to the unique characteristics of each individual company).

164. *See generally* H.R. REP. NO. 73–1383, at 5–6 (1934) (describing the evolving nature of the securities market).

165. *See supra* notes 114–17 and accompanying text (listing several SEC regulations that use the "reasonable investor" standard).

requiring that companies always disclose such events and information upon occurrence.[166] For example, the SEC requires companies that use conflict minerals in the manufacture of its products to disclose whether those minerals originated in the Democratic Republic of the Congo or an adjoining country.[167] Additionally, companies that perform resource extraction must report any payments relating to commercial oil, natural gas, or mineral development made to a foreign government or the Federal Government as a party of their annual disclosures.[168] Finally, the SEC requires companies to disclose the median of the annual total compensation of all employees and the annual total compensation of the company's CEO.[169] In each instance, the SEC provides explicit guidance to facilitate compliance.[170] For example, in the conflict minerals rule, the agency explicitly defines "conflict mineral," listing four minerals and their derivatives.[171]

These bright-line rules demonstrate the SEC's ability to regulate in response to congressional intent, shareholder interests, and external events.[172] In each case, federal officials determined that disclosures addressing societal concerns—such as international relations or disproportionate executive pay—should be made available to all shareholders. While these rules require the SEC to make a larger initial investment in order to provide the higher level of specificity, this greatly reduces the ambiguity and uncertainty as companies prepare their annual reports.[173] Moreover, scholars continue to urge the SEC to expand this pool of exceptions to include information such as a company's CEO's health information.[174] This trend, in combination with the SEC's

166. These requirements have been promoted by mandatory legislation from Congress, but nonetheless demonstrate that specific disclosure requirements are within the SEC's scope of authority.

167. Conflict Minerals, 17 C.F.R. pts. 240, 249b (2018).

168. Disclosure of Payments by Resource Extraction Issuers, 17 C.F.R. pts. 240, 249b.

169. Pay Ratio Disclosure, 17 C.F.R. pts. 229, 249.

170. *But see* BUS. ROUNDTABLE, *supra* note 117, at 1–2 (arguing that deviations from a facts-and-circumstances assessment of materiality wastes SEC resources and buries shareholders in excessive immaterial information).

171. Conflict Minerals, 17 C.F.R. pts. 240, 249b.

172. *See supra* Part I.B (describing the factors that influence the SEC).

173. *See supra* notes 146, 150 and accompanying text (noting the costs and benefits of rules).

174. *See* Tom C. W. Lin, *Undressing the CEO: Disclosing Private, Material Matters of Public Company Executives*, 11 U. PA. J. BUS. L. 383, 383–85 (2009)

willingness to enact rules in certain contexts, implies that the agency may enact a rule in the context of content data breaches. The next Section describes the benefits of a rule requiring disclosure of content data breaches.

C. THE RATIONALE FOR A RULE IN THIS CONTEXT

Data breaches are speculative and occur frequently, causing confusion for companies and difficulty for the SEC in regulating companies—confusion and difficulty that could be eliminated by subjecting breaches to required disclosure. The rate of content data breaches is increasing at an alarming pace.[175] Today, nearly all companies rely on data to grow their business, to improve their products or services, to better understand their customer bases, or to gain insight and manage increasing market complexity and volatility through analytics.[176] In this data-dependent climate, experts believe a company's likelihood of experiencing a data breach is now "inevitable."[177] Companies are increasing

(explaining why a CEO's health is material); *see also* James D. Redwood, *Qualitative Materiality Under the SEC Proxy Rules and the Fifth Amendment: A Disclosure Accident Waiting to Happen or Two Ships Passing in the Night?* 1992 WIS. L. REV. 315, 315 (1992) (arguing that the SEC should require disclosure of un-adjudicated illegal activity under the materiality standard). *See generally* Letter from Dorothy Donohue, Deputy Gen. Counsel, Sec. Regulation of Inv. Co. Inst., to Brent J. Fields, Sec'y, SEC (May 15, 2017), https://www.sec.gov/comments/s7-01-17/s70117-1751450-151844.pdf (responding to the SEC's proposed rule—requiring companies to disclose all material financial obligations, including "default[s] or similar events"—and arguing that the term "event" should specifically include "all defaults, accelerations, terminations, [and] modifications" rather than events that "reflect financial difficulties," as proposed by the SEC). The proposed rule referenced in the letter was 17 C.F.R. § 240.15c2–12.

175. *See supra* notes 37–40 and accompanying text.

176. *See* Hugo Moreno, *Data Analytics Is No Longer a Nice Option—It's the Core of the Enterprise*, FORBES (June 12, 2017), https://www.forbes.com/sites/forbesinsights/2017/06/12/data-analytics-is-no-longer-a-nice-option-its-the-core-of-the-enterprise/#60c0261677ec (surveying and analyzing responses from more than 300 executives across the world and finding that demand for data insights is increasing across all major industries and disciplines).

177. Kyle Balluck, *Corporate Data Breaches 'Inevitable,' Expert Says*, THE HILL (Nov. 30, 2014), https://thehill.com/policy/cybersecurity/225550-cybersecurity-expert-data-breaches-inevitable (recounting an interview with Dave DeWalt, the CEO of Fire Eye—a leading cybersecurity company—stating that ninety-seven percent of all companies are getting breached). DeWalt further stated that hackers are "going to get in . . . But don't let them access the information that's really important. Don't let them get back out with that information. Detect it sooner. Respond sooner. And ultimately that exposure is very small." *Id. See also* Peters, *supra* note 50 (quoting a former assistant chief litigation counsel to the SEC, Matt Rossi, saying, "in the reality that we live in now, cyber breaches are going to be increasingly common").

spending on cybersecurity programs, and investing resources aimed at continual oversight of such programs, but these efforts still do not eliminate the risk of a breach.[178] Charles Kallenbach, a cybersecurity expert and the General Counsel at Heartland Payment Systems, likens a company's database to a nice car, such that companies may lock their databases and hide the keys, yet nothing will keep a persistent thief away.[179]

The speculative substance and form of data breaches, however, render them difficult for companies to manage and for the SEC to regulate.[180] Given the certainty of a breach occurring, the uncertainty that currently exists in how to appropriately respond to a breach is a cause for concern. Consider Equifax: after discovering its breach, the company dedicated forty days to determining the breach's scope and damage, before disclosing the intrusion to Equifax shareholders and to the public.[181] This investigation is largely the product of a materiality standard, which allows for such flexibility in deciding whether to disclose the breach. Requiring disclosure in this context both reflects the benefits of a rule in general[182] and remedies the harms of the

178. *See* Balluck, *supra* note 177 (quoting DeWalt [Fire Eye's CEO], saying, "[t]his isn't a lack of effort. Most companies are growing their security spend"); *see also* Joshua Vaughn, *Into the Breach: Midstate Experts Say Data Breaches Are Inevitable*, SENTINEL (July 20, 2014), https://cumberlink.com/news/local/into-the-breach-midstate-experts-say-data-breaches-are-inevitable/article_6c14ae56-0ebd-11e4-b51c-0019bb2963f4.html (stating that consumer desire for convenience in online shopping and banking has resulted in a state in which breaches and identity theft are inevitable); Jennifer Williams-Alvarez, *At ACC Event, Experts Say Data Breaches Are Inevitable. So Now What?*, CORP. COUNS. (Apr. 14, 2016), https://www.law.com/corpcounsel/almID/1202754933830 (describing: (1) the Association of Corporate Counsel's (ACC's) state of cybersecurity report, which found that fifty-six percent of companies are allocating more money to cybersecurity; and (2) a cybersecurity panel from the ACC's mid-year meeting, at which a panelist stated that "[d]espite the increased awareness of cybersecurity issues, a lot of attacks are still pretty much impossible to prevent").

179. Williams-Alvarez, *supra* note 178. Kallenbach continued with his analogy, stating that his job as an attorney is "to make the neighbor's car look more attractive to take than our car," and urged corporations to take every possible minimal step to protect and to prioritize its data. *Id.*

180. *See* Shawn E. Tuma, *Why Do Data Breach Disclosures Take So Long? Let's Ask the SEC Chairman*, MIS TRAINING INST. (Nov. 13, 2017), https://misti.com/infosec-insider/why-do-data-breach-disclosures-take-so-long-let-s-ask-the-sec-chairman (explaining that companies need "time, effort, and good forensics" to determine the effect of a data breach).

181. *See supra* notes 14–15 and accompanying text.

182. *See supra* notes 142–46 and accompanying text.

materiality standard as specifically applied to corporate disclosure law.[183]

Rules generally increase certainty, decrease official arbitrariness, and provide notice to regulated parties.[184] Accordingly, a rule requiring disclosure in this context would increase certainty and guidance, thereby eliminating the confusion, and facilitate regulated actors' compliance. It would prevent arbitrary delays in regulated companies' disclosure following a breach.[185] To this end, the rule is specific. A company need not disclose every intrusion into its technological domain. As set forth in the Introduction, this Note defines a content data breach as one that compromises at least one thousand records containing consumers' personally identifiable information.[186] This specificity is similar to the SEC's rule that explicitly defines "conflict mineral," listing four minerals and their derivatives.[187] In both cases—the existing rule and this Note's proposed rule—the specificity narrows and focuses the rule's applicability, which minimizes potential imprecision.[188]

Additionally, a rule in this context remedies the concerns of the materiality standard in corporate reporting. The "reasonable investor" standard provides an opportunity for hindsight bias in litigation, the creation of judicial and corporate numerical "rules of thumb," and unequal discretion among firms of different sizes.[189] This rule provides a forward-looking prescription, preventing reliance on additional facts that are otherwise relied upon in litigation, such as empirical evidence, market reactions, and actual significance to the shareholders.[190] For example, in litigation surrounding the fifty-state class action recently filed against Equifax, the court has the ability to reason based off of the actually incurred consequences of the breach.[191] These consequences include the thirty-three percent fall in share price, the

183. *See supra* notes 131–38 and accompanying text.

184. *See supra* Part II.A.

185. *See* Karen Freifeld, *U.S. Companies Allowed to Delay Disclosure of Data Breaches*, THOMSON REUTERS (Jan. 16, 2014), https://www.reuters.com/article/us-target-data-notification/u-s-companies-allowed-to-delay-disclosure-of-data-breaches-idUSBREA0F1LO20140116.

186. *See supra* text accompanying note 27.

187. *See supra* note 171 and accompanying text.

188. *See* Kennedy, *supra* note 139, at 1690 ("[T]he wider the scope of the rule, the more serious the imprecision becomes.").

189. *See supra* notes 131–38 and accompanying text.

190. *See supra* note 131 and accompanying text.

191. *See* Tara Swaminatha, *Equifax Now Hit with a Rare 50-State Class-Action Lawsuit*, CSO (Nov. 22, 2017), https://www.csoonline.com/article/

allegations of insider trading, and the shareholders' determination of significance,[192] each of which is largely irrelevant in litigating the violation of a rule.[193]

Finally, a rule in this context creates an absolute threshold, in turn, removing firms' and courts' undesirable tendency to develop their own rule-of-thumb thresholds for materiality under the "reasonable investor" standard.[194] This further prevents "official arbitrariness" in justifying delays or determining liability.[195] A rule provides an equal disclosure requirement for all firms, regardless of its size and "total mix" of information.[196] This would prevent larger firms from enjoying greater flexibility than smaller companies in deciding when and whether to report a data breach.[197]

Companies today are often global entities, as the internet allows an international presence from a local base.[198] The speculative nature of data breaches—in both a breach's scope and source and in whether or not to disclose—in combination with a patchwork of state reporting regulations[199] and a vague federal reporting standard results in confusion. This confusion is then reflected in a company's reporting conduct. The SEC has acknowledged this confusion and attempted to provide guidance twice in the past, to no avail.

3238076/data-breach/equifax-now-hit-with-a-rare-50-state-class-action-lawsuit.html (discussing the details of the complaint); *see also supra* note 24 and accompanying text.

192. *See supra* notes 2, 16–19 and accompanying text.

193. *See* Sunstein, *supra* note 139, at 962.

194. *See supra* notes 132–34 and accompanying text.

195. *See supra* note 143 and accompanying text.

196. *See supra* notes 137–38 and accompanying text.

197. *See supra* notes 135–38 and accompanying text.

198. *See* Nataly Kelly, *Taking Your Brand Global Is Easier than You Think*, HARV. BUS. REV. (Aug. 23, 2013), https://hbr.org/2013/08/taking-your-brand-global-is-ea (describing the process of going global as a "path," rather than an "obstacle course").

199. *See, e.g.*, Andrea Peterson, *Privacy Advocates: A National Data Breach Notification Standard Might Actually Make Things Worse*, WASH. POST (Jan. 12, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/01/12/privacy-advocates-a-national-data-breach-notification-standard-might-actually-make-things-worse/?utm_term=.9dadcab2c500 (explaining that today, forty-seven states have enacted security breach notification laws).

D. EXISTING GUIDANCE IS INSUFFICIENT

In 2011, the SEC issued guidance to address this confusion, instructing companies to discuss cybersecurity threats and incidents in management's discussion and analysis of financial condition and results of operations (MD&A)[200]—a section of their annual reports.[201] In reality, the SEC's guidance statement contained only abstract direction[202] and proved relatively ineffective in subsequent corporate reporting.[203] Even with perfect compliance, a company may wait several months before disclosing a data breach at their next annual filing, such as Equifax's forty-day delay.[204] During that waiting time, the company is incurring excessive costs to remediate the breach and increase security, as well as diverting resources toward the breach which otherwise may be directed toward furthering other business objectives.[205]

On February 26, 2018, the SEC released additional guidance to address the disclosure of data breaches.[206] The guidance acknowledged several concerns and recognized several costs of data breaches that this Note has described.[207] Furthermore, the

200. *See id.*

201. *See* Commission Guidance Regarding Management's Discussion and Analysis of Financial Condition and Results of Operations, 68 Fed. Reg. 75,056, 75,056 (Dec. 29, 2003) (codified at 17 C.F.R. pts. 231 and 241) (stating that MD&A requirements are intended to satisfy three objectives: "[(1)] To provide a narrative explanation of a company's financial statements that enables investors to see the company through the eyes of management; [(2)] [t]o enhance the overall financial disclosure and provide the context within which financial information should be analyzed; and [(3)] [t]o provide information about the quality of, and the potential variability of, a company's earnings and cash flow, so that investors can ascertain the likelihood that past performance is indicative of future performance.").

202. *See* Press Release, SEC, *supra* note 49 (acknowledging that the 2011 guidance statement was "principles based").

203. *See* Freifeld, *supra* note 185 (quoting a former acting assistant attorney general at the U.S. Justice Department saying that since the 2011 guidance document was issued, "companies have tended to include generic risk factors rather than disclose specific incidents"); *see also, e.g.*, Laura Northrup, *Did Yahoo Wait Too Long to Disclose Massive 2014 Data Breach? SEC Investigating*, CONSUMERIST (Jan. 23, 2017), https://consumerist.com/2017/01/23/did-yahoo-wait-too-long-to-disclose-massive-2014-data-breach-sec-investigating (reporting that Yahoo experienced breaches in 2013 and 2014, but failed to disclose the breaches until 2016).

204. *See supra* note 15 and accompanying text.

205. *See supra* Part III.B (discussing the negative impacts of a data breach on a company).

206. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8166, 8166 (Feb. 26, 2018) (to be codified at 17 C.F.R. pts. 229 and 249) [hereinafter 2018 Guidance].

207. *Id.* at 8166–67.

guidance explains that a cybersecurity incident's materiality depends upon the incident's nature, extent and potential magnitude, as well as the incident's range of potential harm to a company's reputation, financial performance, and customer and vendor relationships.[208] Although perhaps more specific than the 2011 guidance, this direction does not provide any more clarity than what previously existed. Instead, it lists every obvious factor that could be relevant to a company's decision to disclose a data breach, and instructs the company to "make appropriate disclosure timely and sufficiently prior to the offer and sale of securities."[209]

Despite its recognizing the gravity of data breaches, the 2018 guidance leniently concedes that determining the implications of a cybersecurity incident may require time, thus excusing reporting delays such as Equifax's forty-day delay.[210] In sum, this guidance kicks the can down the road. It encourages companies to continue reporting data breaches in the manner in which they are already reporting.[211] Importantly, however, one of these manners is the Form 8-K, which the SEC "encourages companies to continue to use" to report cybersecurity incidents.[212] In the guidance, the SEC states that it continues to "consider other means of promoting appropriate disclosure of cyber incidents."[213] One such means, providing the most appropriate disclosure, is a rule mandating disclosure of content data breaches on a Form 8-K, a vehicle of disclosure that the SEC has now formally endorsed.

III. THE RULE IN PRACTICE: PROTECTING INVESTORS AND PROMOTING TRANSPARENCY

This Part explores the details of the rule and its potential impact. It argues that required disclosure of content data breaches furthers the purposes of corporate disclosure laws and promotes informed investment by increasing transparency. Finally, this Part addresses likely concerns with the proposed rule.

208. *Id.* at 8169.
209. *Id.*
210. *Id.*
211. *Id.* at 8168–69 (providing examples of current content data breach reporting options).
212. *Id.* at 8168.
213. *Id.* at 8167.

A. THE RULE

This Note proposes the following rule: companies subject to SEC regulations must disclose content data breaches as material impairments within four days of discovery by way of the SEC's Form 8-K (hereinafter referred to as the Content Data Breach Disclosure Rule, or CDBD Rule). For purposes of this Note "content data breach" is defined as a data breach that has compromised at least one thousand records containing consumers' personally identifiable information.

Several definitions of a data breach exist, though all are variations of a theme describing a "confirmed incident in which sensitive, confidential or otherwise protected data has been accessed and/or disclosed in an unauthorized fashion."[214] The CDBD Rule embraces the notions of unauthorized access and compromised data, while quantitatively limiting the scope of the rule's applicability. The limitation recognizes the reality that data breaches are not always dramatic infiltrations by malicious hackers.[215] The numerical threshold—1000 records—aims to eliminate the risk of requiring company disclosure for day-to-day breaches.[216] As mentioned in the Introduction, this number comes from a Ponemon Institute study, sponsored by IBM Security, (hereinafter referred to as the "Ponemon Study") that defines a material data breach as "one that involves a minimum of 1,000 lost or stolen records containing personal information about consumers or customers."[217] The Ponemon Study is well-respected and often cited by technology companies and cybersecurity experts when discussing various aspects of data breaches.[218] Nonetheless, this number remains a somewhat arbitrary threshold, and thus provides an opportunity for future work and input from cybersecurity experts.

214. *Data Breach*, TECHTARGET, https://searchsecurity.techtarget.com/definition/data-breach (last visited Mar. 10, 2019); *see also, e.g.*, *Data Breach*, TREND MICRO, https://www.trendmicro.com/vinfo/us/security/definition/data-breach (last visited Mar. 10, 2019) (defining data breach as "an incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner").

215. *See* TECHTARGET, *supra* note 214 (explaining that a hack can be as innocent as an unauthorized hospital employee reading a patient's health information over the shoulder of an authorized hospital employee).

216. *See id.*

217. PONEMON STUDY, *supra* note 27, at 2.

218. *See, e.g.*, Michael Bruemmer, Data Breach Resolution Grp., Vice President, *Survey—Most Companies Ill-Prepared for a Global Data Breach*, EXPERIAN (June 27, 2017), http://www.experian.com/blogs/data-breach/2017/06/27/survey-companies-ill-prepared-global-data-breach/; *New Study: Data Theft*

Personally identifiable information (PII) is a familiar concept throughout privacy law, including state data breach notification laws.[219] The CDBD Rule takes advantage of this familiarity, defining PII as "any piece of information which can potentially be used to uniquely identify, contact, or locate a single person."[220] This can include street addresses, device IP addresses, phone numbers, social security numbers, driver's licenses, and vehicle registrations.[221] PII's presence throughout federal and state laws captures its general acceptance as an appropriate benchmark in the technological domain.[222] Additionally, the Ponemon Study employs PII in its definition of "data breach," demonstrating the cybersecurity industry's acceptance of this term.[223]

In sum, the CDBD Rule incorporates recognized and appropriate terms and definitions. This familiarity prevents the rule from surprising corporations. Companies can measure one thousand records and identify records containing PII. This ultimately reflects the benefits of a rule-based approach, replacing uncertain reporting standards with concrete definitions and thresholds.[224] Moreover, the rule itself operates to protect investors and increase transparency, ultimately achieving the purposes of corporate disclosure.

Rising Sharply, Insider Threats Cited as Leading Cause, VARONIS (Aug. 9, 2016), http://ir.varonis.com/news-releases/news-release-details/new-study-data-theft-rising-sharply-insider-threats-cited.

219. *See, e.g.*, Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2012); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (1988); Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 MASS. CODE REGS. § 17.00–.05 (2010).

220. *Financial Services Compliance*, INTRUSION, http://www.intrusion.com/index.php?option=com_content&view=article&id=29&Itemid=40 (last visited Mar. 10, 2019).

221. *See id.*

222. *See* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1819–21 (2011) (discussing the rise of PII's significance throughout the last fifty years).

223. *See* PONEMON STUDY, *supra* note 27, at 2.

224. *See supra* Part II.A.

B. PROTECTING INVESTORS BY ACKNOWLEDGING SHAREHOLDER HARM

The SEC was created in order to advance the purposes of the Securities Act and the Exchange Act.[225] These Acts aim to promote transparency in order to enhance informed investments, and ultimately, to protect the investors.[226] Purchasing stock is one vehicle for the public to invest in a company.[227] As such, a company's stock share price is a direct reflection of a shareholder's investment, and thus, his or her interest.[228] While an increase in share price benefits the shareholder, a decrease in share price harms the shareholder. When this harm is created or accompanied by a lack of corporate transparency, it offends and runs counter to the purposes of the Securities Act and the Exchange Act. Content data breaches are corporate events that often decrease a company's stock price. Therefore, shareholder harm resulting from content data breaches requires SEC remediation. The CDBD Rule serves as such remediation.

The effects of a content data breach, including direct and indirect costs, were discussed in Part I, above.[229] These types of damages and harms trigger disclosure under Form 8-K. In the 2004 Rule, the SEC states that Item 2.06 requires disclosure when a company concludes that there has been a "material charge for impairment to one or more of its assets, including, without limitation, an *impairment of securities or goodwill*."[230] A content data breach impairs both securities, evidenced by an immediate and extended decrease in stock price and direct costs of a data breach,[231] and goodwill, evidenced through the indirect costs of a data breach.[232] These impairments harm shareholders directly—by decreasing the value of the company[233]—and indirectly—by diverting costs from growth or strategic progress, and decreasing shareholder trust.

225. *See supra* Part I.A.

226. *See supra* notes 80–85 and accompanying text.

227. *See supra* note 77 and accompanying text.

228. *See* Mauboussin, *supra* note 77.

229. *See supra* Part I.A; *see also* Mark S. Johnson et al., *Stock Price Reaction to Data Breaches*, 16 J. FIN. ISSUES 1, 11 (2017) (finding an average .37% decrease in firm equity value following a data breach).

230. 2004 Rule, *supra* note 101 (emphases added).

231. *See supra* notes 41–65 and accompanying text.

232. *See supra* notes 66–71 and accompanying text.

233. *See* Brian Palmer, *Watch Out for Falling Stock Prices*, SLATE (Aug. 9, 2011), https://www.slate.com/news-and-politics/2011/08/does-it-matter-to-a

Considering that corporate disclosures strive to protect investors, these harms should be reported as early as possible. To be clear, this Note does not take the position that the CDBD Rule will necessarily remedy the costs of a data breach, but rather that these costs harm investors, and thus, a company is obligated to inform its investors of a content data breach. Historically, the SEC has acted to protect investors in response to external events that make certain information more relevant to a company's shareholders.[234] The era of content data breaches, and its corresponding effect on shareholder interests, is precisely the type of event that should trigger SEC action.

C. PROMOTING INFORMED INVESTMENT BY INCREASING CORPORATE TRANSPARENCY

The CDBD Rule would resolve existing confusion and concern among companies, attorneys, and accountants regarding cybersecurity-related disclosure.[235] The Form 8-K requires companies to report material impairments within four days of a triggering event.[236] When the SEC amended Form 8-K in 2004, the agency expanded the Form's scope in order to prevent the delayed disclosure that existed under the previous Form 8-K, aiming to benefit investors by "assimilat[ing] such undisclosed information into the value of a company's securities."[237] Per the CDBD Rule, required disclosure within four days would provide investors with transparency during the company's entire recovery period. The SEC's lenient approach may have been appropriate in the past, when the market was first facing concerns related to cybersecurity incidents, but that time has since passed.[238] Congress established the SEC in order to regulate in

-company-if-its-stocks-lose-value.html (explaining that when a stock price decreases, shareholders "clearly tak[e] a major hit, since they own the stocks").

234. *See supra* Part I.B.

235. *See CF Disclosure Guidance: Topic No. 2*, SEC (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm ("Recently, there has been increased focus by registrants and members of the legal and accounting professions on how these [cybersecurity] risks and their related impact on the operations of a registrant should be described within the framework of the disclosure obligations imposed by the federal securities laws.").

236. *See* FORM 8-K, *supra* note 35, at 2.

237. *See* 2004 Rule, *supra* note 101, at 15,594.

238. *See* Ezequiel Minaya, *SEC Says Companies Can Expect New Guidelines on Reporting Cybersecurity Breaches*, WALL ST. J. (Nov. 9, 2017), https://www.wsj.com/articles/sec-says-companies-can-expect-new-guidelines-on-reporting-cybersecurity-breaches-1510267201 (describing a senior SEC regulator's warn-

accordance with changing times and provided it with the flexibility and resources necessary to target developments such as the inevitability of data breaches.[239]

Periodic reporting and Form 8-K allow companies to continually provide the public with important information as it arises. By creating the CDBD Rule, the SEC would provide transparency with regard to a prominent corporate issue—content data breaches.[240] This transparency may operate to increase investor confidence in the market,[241] in turn, reducing the amount of speculation relating to cybersecurity incidents.[242] Under existing circumstances, shareholders are largely uncertain of how to respond to data breach and often sell their shares in a panic, attempting to distance themselves from the breached company.[243] In this context, mandated disclosure through the CDBD Rule would reveal the true prevalence of data breaches,[244] which perhaps would diminish shareholders' instinctual hostile reaction and provide more rational market reactions to data breaches. In return, this may reduce companies' resistance to fully and transparently disclosing data breaches in the future, providing more rational market reactions.

Greater transparency, greater confidence, and reduced speculation would ultimately encourage capital formation, investment, and growth in this country's economic state.[245] Even if such lofty hopes are unavailing, a rule requiring disclosure of

ing that the "spate of high-profile breaches" has prompted the need for new directions regarding data breach disclosure laws); *see also supra* notes 37–76 and accompanying text (discussing the recent increase in cybersecurity incidents).

239. *See* H.R. REP. NO. 73-1383, at 6–7 (1934) (explaining that despite Congress's overall desire to limit agency discretion, in securities—"a field where practices constantly vary"—broad discretion is "practically essential").

240. *See supra* notes 175–79 and accompanying text.

241. *See* H.R. REP. NO. 73-1383, at 11 ("There cannot be honest markets without honest publicity. Manipulation and dishonest practices of the market place thrive upon mystery and secrecy.").

242. *See* Tuma, *supra* note 180.

243. *See* Kvochko & Pant, *supra* note 41 (stating that shareholders lack both information about cybersecurity incidents generally and tools to measure the resulting impact of the breach); *accord* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 753–54 (2018) (illustrating that the harms of data breaches are difficult to conceptualize and articulating claims that breaches cause consumers anxiety and emotional distress).

244. *See supra* notes 175–79 and accompanying text.

245. *See What We Do*, *supra* note 78 (explaining that disclosure promotes a "more active, efficient, and transparent capital market that facilitates the capital formation so important to our nation's economy").

content data breaches nonetheless facilitates informed investing. At a minimum, a rule will provide investors important, relevant information as they navigate the securities market, allowing an investor to form an "intelligent basis for forming his judgment as to the value of the securities he buys or sells."[246] Thus, the rule facilitates informed investments, which directly satisfies President Roosevelt's directive to Congress in 1933,[247] and Congress's hopes for the Exchange Act.[248]

D. REJECTING OBJECTIONS

Companies often postpone reporting a content data breach.[249] At the time of disclosure, companies justify this delay by explaining it was investigating and identifying the accurate scope and damage of the breach, attempting to avoid premature disclosure.[250] In its 2018 guidance, the SEC accepts these investigations and disclosure delays as understandable.[251] This argument embodies the speculative nature of content data breaches, as companies attempt to avoid premature disclosure, preferring instead to have as many facts as possible before publicly reporting the incident.[252] Accordingly, the SEC's 2004 proposed amendments to Form 8-K were met with opposition. In response to Item 2.06, commentators noted that material impairments "can occur over time, making it difficult to determine the exact date of the triggering event."[253] Moreover, commentators believed the annual reports were better suited to address these events, because discussing a single piece of information outside of the context of the entire financial statements would be "difficult and potentially misleading."[254] The SEC, however, was not convinced.

246. *See* H.R. REP. NO. 73-1383, at 11.

247. *See supra* text accompanying note 80.

248. *See* H.R. REP. NO. 73-1383, at 5 (listing the causes of "dangerous speculation" in the securities market, including "inadequate corporate reporting which keeps in ignorance of necessary factors for intelligent judgment of the values of securities a public continually solicited to buy such securities by the sheer advertising value of listing").

249. *See infra* note 275 and accompanying text.

250. *See, e.g.*, Press Release, Equifax, *supra* note 9.

251. 2018 Guidance, *supra* note 206, at 8169.

252. *See* Tuma, *supra* note 180 (explaining that preparing disclosures is difficult and subjective, and thus, without adequate time to investigate the facts, disclosures may be misleading).

253. 2004 Rule, *supra* note 101, at 15,601.

254. *Id.*

The agency responded to these concerns by stating that it believes it is "important for investors to receive this information on a current basis."[255] This response reflects Congress's intent to prioritize transparency and promote informed investment.[256] The SEC further stated that by tying the reporting deadline to the board's, a committee's, or an officer's discovery of a content data breach, the timing of disclosure is "sufficiently precise."[257] Over a decade later, the SEC continues to endorse companies' using a Form 8-K to disclose data breaches.[258] Nonetheless, the SEC acknowledged in its Final 2004 Rule that the discovery of a data breach can often occur in conjunction with preparing, reviewing, or auditing financial statements during the development of periodic reports.[259] Thus, if a company discovers a content data breach while preparing quarterly or annual reports and it plans to disclose the breach in the relevant report, then Form 8-K disclosure is not required[260] and the CDBD Rule would not be triggered. Beyond such circumstances, the SEC was, is, and should be unwilling to sympathize with the commentators' concerns.

Moreover, existing sources of regulation mitigate commentators' concerns by demonstrating the capability of rapid disclosure. As the threat and inevitability of data breaches has gained increased recognition, various regulatory bodies have instituted reporting deadlines for cybersecurity incidents.[261] For example, Europe's new General Data Protection Regulation (GDPR) establishes a seventy-two hour—or three-day—reporting deadline for data breaches.[262] The GDPR—effective May 25, 2018—requires entities to disclose any discovered breach within seventy-two hours, unless the breach is "unlikely to result in a risk to the rights and freedoms of natural persons."[263] Similarly, in 2017,

255. *Id.*

256. *See supra* Part III.C.

257. 2004 Rule, *supra* note 101, at 15,601.

258. 2018 Guidance, *supra* note 206, at 8168.

259. *See id.*

260. *See id.*

261. *See* Freifeld, *supra* note 185 (describing state disclosure laws, some of which—including Florida, Vermont, and Wisconsin—have established specific forty-five-day disclosure deadlines for data breaches).

262. Council Regulation 2016/679, art. 33(1), 2016 O.J. (L 119).

263. *Id.*; *see also GDPR and 72-Hour Breach Reporting: What You Need to Know*, ZONE FOX: BLOG (Apr. 10, 2017), https://www.zonefox.com/blog/gdpr-and-72-hour-breach-reporting-what-you-need-to-know (explaining the nuts and bolts of the seventy-two-hour requirement).

New York became the first state to implement detailed regulations applicable to financial services entities, including banks, insurance companies, brokers, and others.[264] This regulation—effective March 1, 2017—requires covered entities to take certain proactive measures, including reporting all cybersecurity events and breaches to the Department of Financial Services within seventy-two hours.[265] Inspired by New York's regulation, the National Association of Insurance Commissioners adopted a seventy-two hour reporting deadline in October, 2017, for any cybersecurity event resulting in "unauthorized access to, disruption or misuse of, an Information System or information stored on such Information System."[266]

These reporting deadlines not only signal the increased urgency in requiring disclosure of cybersecurity incidents, but also demonstrate that despite the speculative nature of data breaches, immediate disclosure is in fact possible. For example on October 5, 2017, a security expert notified an online commenting system, Disqus, that it had been breached in 2012.[267] Within just twenty-four hours, Disqus had contacted possibly-affected users and disclosed the breach to the public.[268] In the face of new regulations and reporting deadlines, one can hardly argue that Disqus is an anomaly, such that its rapid disclosure is not replicable by others. Instead, companies everywhere must likewise prioritize these reporting responsibilities. As corporations today can reach further with fewer resources,[269] centralized regulation is likely most effective. Accordingly, the centralized SEC is the appropriate body to unify corporate reporting practices with regard to content data breaches by way of the CDBD Rule.

CONCLUSION

Corporate disclosure law has historically been viewed as a framework, or patchwork, of vague requirements, rules, and regulations.[270] This view rings true in the field of cybersecurity.

264. N.Y. COMP. CODES R. & REGS. tit. 23, § 500.01 (2018).

265. *Id.* § 500.17.

266. INSURANCE DATA SECURITY MODEL LAW § 3(D) (NAT'L ASS'N INS. COMM'RS 2017).

267. *See* Eduard Kovacs, *Disqus Discloses 2012 Breach Impacting 17 Million Users*, SECURITY WK. (Oct. 9, 2017), https://www.securityweek.com/disqus-discloses-2012-breach-impacting-17-million-users.

268. *See id.*

269. *See supra* note 198 and accompanying text.

270. *See, e.g.*, Oesterle, *supra* note 118, at 168 (stating that the SEC rests many federal securities laws on the notion of materiality without defining the

Technology continues to develop and companies continue to incorporate this developing technology into their business and operations. In the face of these developments, the rate of content data breaches is rising.[271] In this field, disclosure is muddied by an inarticulate standard of materiality, an issue that is engulfing the corporate domain, with no further guidance from the SEC.[272]

Content data breaches provide the SEC with the opportunity to resolve a small amount of the overwhelming ambiguity. They are a discrete issue. They are capable of objective identification. They are destructive. They are material events which should mandate disclosure to the public. The CDBD Rule, requiring disclosure of content data breaches as material impairments under Item 2.06 of Form 8-K, will increase transparency in the capital market. This proposition finds its basis in President's Roosevelt instruction to Congress in 1933 to decrease speculation in the marketplace.[273] It finds support in its advantages in comparison to an unclear standard.[274] Finally, this solution finds its benefit in its practical application—protecting investors and enhancing informed investment.[275] This requirement provides a more secure and reliable market, ultimately fueling investments and strengthening corporate America.

term, thus leading academics to critique the standard as too vague).

271. *See supra* notes 37–76 and accompanying text.

272. *See supra* notes 235–38 and accompanying text.

273. *See supra* Part I.A.

274. *See supra* Part II.C.

275. *See supra* Parts III.B & III.C.