HACKING OUR SECURITIES DISCLOSURE SYSTEM: THE NEED FOR FEDERAL BROKER-DEALER DISCLOSURE REQUIREMENTS VIS-À-VIS CYBER INCIDENTS

Jason Auman*

Broker-dealers provide investors with the platform to access security markets. To facilitate this access, clients entrust them with sensitive information, including their names, addresses, and social security numbers. Cyberattacks on the financial sector have advanced in sophistication and grown more frequent due to technological advances, adjustments in firm business models, and changes in customer behavior, causing new vulnerabilities in firm information systems. However, even with this increase of cyberattacks against broker-dealers, the lack of public disclosure requirements means little is known about the extent of broker-dealer cyber safety.

Under current SEC regulations, broker-dealers must take preventative action, such as establishing safeguards against cyber breaches and maintaining security programs that can identify red flags. However, after a cyberattack occurs, firms are only required to file a Suspicious Activity Report to FinCEN, a bureau within the Treasury Department. Unlike public companies and banks, broker-dealers do not have any federal disclosure requirement to the general public for cybersecurity incidents. Addressing this gap requires a comprehensive examination of the tradeoffs involved in

* J.D. Candidate 2019, Columbia Law School; B.S. 2015, Yeshiva University. Many thanks to Professor Joshua Mitts for his invaluable guidance and feedback. Additional thanks to the editorial staff of the *Columbia Business Law Review* for their diligent work and assistance in preparing this Note for publication. All errors are my own.

implementing broad new federal disclosure requirements for broker-dealers following cybersecurity incidents.

I. INTRODUCTION

Broker-dealers provide investors with a platform to access securities markets. Their clients entrust them with sensitive information including names, addresses, social security numbers, and even financial information, such as annual

income and net worth.[1] However, according to a 2015 Securities and Exchange Commission ("SEC") report, eighty-eight percent of broker-dealers have been the victims of cyberattacks, a significant number of which involved losses of over $5000.[2] Moreover, cyberattacks in the financial sector have grown more frequent and sophisticated due to technological advances, adjustments in firm business models, and changes in how customers use technology, each of which cause new vulnerabilities in firm information systems.[3] Other than a handful of famous data breaches, such as those involving Fidelity in 2014[4] and TD Ameritrade in 2007,[5] a lack of public disclosure requirements means that little is known about the extent of broker-dealer cyber safety.[6]

Under current SEC regulations, broker-dealers must take preventative actions like establishing safeguards against cyber breaches and maintaining security programs that can identify red flags.[7] These include adopting policies and procedures to protect customer information and to detect,

1 *What to Expect When You Open a Brokerage Account*, FIN. INDUS. REGULATORY AUTH., http://www.finra.org/investors/what-expect-when-you-open-brokerage-account [https://perma.cc/2349-WW8N].

2 *See* Office of Compliance Inspections and Examinations, *Cybersecurity Examination Sweep Summary*, SEC NAT'L EXAM PROGRAM RISK ALERT, Feb. 3, 2015, at 2–3, https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf [https://perma.cc/SVR6-C6Q7].

3 FINRA, REPORT ON CYBERSECURITY PRACTICES 1 (2015), https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf [https://perma.cc/XF8E-Z9XB].

4 Danielle Walker, *JPMorgan Hackers Targeted 13 Firms, Including Fidelity, Report Reveals*, SC MEDIA (Oct. 10, 2014), https://www.scmagazine.com/jpmorgan-data-breach-targeted-fidelity-12-others/article/540011/ [https://perma.cc/5A85-8KXP].

5 Dawn Kawamoto, *TD Ameritrade's 6 Million Customers Hit with Security Breach*, CNET (Nov. 26, 2007, 3:42 PM), https://www.cnet.com/news/td-ameritrades-6-million-customers-hit-with-security-breach/ (on file with the *Columbia Business Law Review*).

6 *See infra* text accompanying notes 57–59.

7 *See infra* Section II.C.1.

prevent, and mitigate identity theft.[8] Once a serious cyberattack occurs, the firm's only obligation is to file a Suspicious Activity Report with the Financial Crimes Enforcement Network ("FinCEN"), a bureau within the Treasury Department.[9] Unlike public companies and banks, no federal disclosure requirement mandates that broker-dealers notify the general public about cybersecurity incidents.[10] States have started to fill in the gap with a patchwork of regulation.[11] Notably, New York, Vermont, and Colorado each enacted different schemes for addressing cyber-risks and breaches.[12] Most states also have statutes requiring that companies disclose breaches compromising their residents' social security numbers and credit card information.[13] However, these laws are broadly applied and are not tailored to the specific needs of the broker-dealer industry. This Note argues that this lacuna in the regulatory framework should be addressed by applying specific federal disclosure requirements to broker-dealers for cybersecurity incidents.

Part II of this Note provides the regulatory backdrop of cybersecurity disclosure requirements. Specifically, Part II reviews the contrasting requirements imposed by regulators on public companies and banks, and then examines the federal, state, and international requirements currently in place for broker-dealers. Part III identifies the unique characteristics of broker-dealers that must be taken into account when addressing cybersecurity incidents. Part IV presents potential solutions and proposes federal disclosure requirements which specifically address broker-dealer concerns. Part V offers concluding remarks.

8 *See infra* text accompanying note 71.

9 *See infra* Section II.C.3.

10 *See infra* text accompanying notes 57–59.

11 *See infra* Section II.D.

12 *See infra* Section II.D.1.

13 *See infra* Section II.D.2.

II. THE CURRENT CYBERSECURITY DISCLOSURE REQUIREMENTS

Regulators protect consumers through different regulatory schemes, depending on the type of financial entity entrusted with the consumers' information. This Part explores the various ways in which regulators protect consumer data. Sections II.A and II.B examine the discrepancy between the regulations that are geared toward public companies versus banks. Section II.C provides an overview of the current federal cybersecurity regulations imposed on broker-dealers. Section II.D describes recently enacted state disclosure legislation that broadly impacts all financial entities. Section II.E briefly provides some international background, comparing the regulatory requirements in the United States with recent regulatory changes in the European Union.

A. Public Company Materiality Standard

The basis of the SEC's public company regulatory regime is disclosure. During the Great Depression, Congress passed the Securities Act of 1933[14] and the Securities Exchange Act of 1934,[15] two important statutes enacted to regulate the securities markets and limit manipulative activities therein.[16] The Securities Act of 1933 created the SEC, whose stated mission is to "protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation."[17] However, instead of endowing the SEC with more substantive responsibilities,[18] the Act primarily focuses on

14 15 U.S.C. § 77a (2012).

15 *Id.* § 78a.

16 *See* Elisabeth Keller & Gregory A. Gehlmann, *Introductory Comment: A Historical Introduction to the Securities Act of 1933 and the Securities Exchange Act of 1934*, 49 OHIO ST. L.J. 329, 342–51 (1988).

17 *What We Do*, U.S. SEC. & EXCHANGE COMMISSION, http://www.sec.gov/about/whatwedo.shtml#.U_UePRZ7Tww [https://perma.cc/VL4W-SXZ5] (last modified June 10, 2013).

18 In contrast to the SEC's disclosure regime, many state-level blue sky statutes grant state regulators the power to conduct "merit

mandatory disclosure requirements for public companies to enable investors to make sound investment decisions.[19] To that end, the SEC requires companies to file annual 10-K Forms,[20] quarterly 10-Q Forms,[21] and 8-K Forms after the occurrence of specified triggering circumstances, such as a bankruptcy or a change in the company's certifying accountant.[22]

Companies are not required to disclose all information; the requirement is limited by a materiality standard.[23] Companies only must disclose "matters to which there is a substantial likelihood that a reasonable investor would attach importance in determining whether to purchase the security registered."[24] The Supreme Court has further clarified the materiality standard, requiring that "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 made available."[25] The materiality standard provides investors with all relevant and necessary information so that they will have a rational basis upon which to make investment decisions.[26] This democratization of information,

regulation." Roberta S. Karmel, *Blue-Sky Merit Regulation: Benefit to Investors or Burden on Commerce?*, 53 BROOK. L. REV. 105, 105 (1987). These reviews are substantive in nature and allow the regulator to prevent a sale of securities in the state "when the offering or the issuer's capital structure is substantively unfair or presents excessive risk to the investor." *Id.*

19 *See* Alan B. Levenson, *The Role of the SEC as a Consumer Protection Agency*, 27 BUS. LAW. 61, 62 (1971).

20 *See* 17 C.F.R. § 249.310 (2018).

21 *See id.* § 240.13a-13.

22 *See id.* § 240.13a-11; *Form 8-K*, U.S. SEC. & EXCHANGE COMMISSION, https://www.sec.gov/fast-answers/answersform8khtm.html [https://perma.cc/HL6M-VSNR] (last modified Aug. 10, 2012).

23 *See* Levenson, *supra* note 19, at 62, 65.

24 17 C.F.R. § 230.405 (2018).

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

26 Levenson, *supra* note 19, at 62.

policymakers believe, will ensure a fair and efficient market and enhance corporate governance.[27]

Although the materiality standard may have applied to corporate risks (including cybersecurity matters) prior to 2011, many companies did not report cybersecurity information in their public filings, and the SEC had not issued specific guidance on the topic.[28] According to a 2009 survey by insurance company Hiscox, "[t]hirty-eight percent of Fortune 500 companies [surveyed] fail to acknowledge the threat of a data breach in the Risk Factors section of their SEC 10-K filing."[29] The report adds that "of the companies that do include the risk of a data breach in their 10-K, 26 percent fail to mention the consequential financial impact while a further 49 percent failed to identify the reputational impact."[30] As SEC Commissioner Mary Jo White explained, "[w]hen the Commission adopted rules decades ago requiring a description of the company's business, risk factor disclosure and [management discussion & analysis], there were no such things as smartphones, tablets, or even the internet. And, so the SEC was not thinking about the risks presented by cybersecurity attacks or breaches."[31]

---

[27] *See id.*; *see also* Henry T. C. Hu, *Too Complex to Depict? Innovation, "Pure Information," and the SEC Disclosure Paradigm*, 90 TEX. L. REV. 1601, 1606 (2012).

[28] *See* Press Release, Hiscox, U.S. Companies Still Underestimate Impact of Data Breaches, Says Hiscox Report [hereinafter Hiscox Report], http://www.hiscoxgroup.com/news/press-releases/archive/2009/22-04-09.aspx?p=1 [https://perma.cc/3REC-C7RW]; *see also* Letter from John D. Rockefeller IV, Chairman, U.S. Senate Comm. on Commerce, Sci., & Transp., Robert Menendez, U.S. Senator, Sheldon Whitehouse, U.S. Senator, Mark Warner, U.S. Senator, & Richard Blumenthal, U.S. Senator, to Mary Schapiro, Chairman, SEC (May 11, 2011), https://www.slideshare.net/100fsteet/letter-from-senator-rockefeller-to-sec-chairman-schapiro-regarding-cyber-security-disclosure-may-2011 [https://perma.cc/6TPL-6EJU].

[29] Hiscox Report, *supra* note 28.

[30] *Id.*

[31] Mary Jo White, Chair, SEC, The Path Forward on Disclosure, Address to the National Association of Corporate Directors (Oct. 15, 2013) (transcript available at https://www.sec.gov/news/speech/spch101513mjw [https://perma.cc/DH8T-LYH4]).

In October 2011, the SEC responded with guidelines for public companies' cybersecurity disclosure responsibilities.[32] SEC Commissioner White explained, "[e]ven though cybersecurity attacks were not specifically contemplated, the disclosure requirements generally cover these risks. That is because, even in the absence of a line item requirement, the basic standard of 'materiality' governs. Depending on the severity and impact of the cybersecurity attacks, disclosure is either required or not."[33] The guidance examines the various sections that are currently disclosed in a Form 10-K—risk factors, management's discussion and analysis ("MD&A"), description of business, legal proceedings, financial statement disclosures, and disclosure controls and procedures—and explains the cybersecurity risks a company must consider in each corresponding section of its disclosures.[34]

Regarding risk factors, the guidance advises disclosing the risk of cyber incidents "if these issues are among the most significant factors that make an investment in the company speculative or risky."[35] This criterion did not provide much clarity, though, as the requirement is identical to the normal materiality threshold for reporting risk factors.[36] The guidance further instructs companies to address cybersecurity risks in their MD&A section, just as the normal materiality threshold:

---

[32] *See* SEC, CF DISCLOSURE GUIDANCE: TOPIC NO. 2 (2011), http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm [https://perma.cc/XH5N-HHDU]. The SEC announced in November 2017 that it would seek even stricter cybersecurity disclosure requirements. *See generally* Ezequiel Minaya, *SEC Says Companies Can Expect New Guidelines on Reporting Cybersecurity Breaches*, WALL ST. J. (Nov. 9, 2017, 5:40 PM), https://www.wsj.com/articles/sec-says-companies-can-expect-new-guidelines-on-reporting-cybersecurity-breaches-1510267201 (on file with the *Columbia Business Law Review*).

[33] White, *supra* note 31.

[34] *See* SEC, *supra* note 32.

[35] *Id.*

[36] *See* 17 C.F.R. § 229.503(c) (2018).

> if the costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant's results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition.[37]

The guidance instructs companies to include information in the business description section if a cyber incident materially affects products, services, customer relationships, or competitive conditions.[38] Similarly, companies should disclose legal proceedings related to cyber incidents and costs related to cyber incidents in the financial statement disclosures section if they are considered material "depending on the nature and severity of the potential or actual incident."[39] Finally, companies must report disclosure controls and procedures "[t]o the extent cyber incidents pose a risk to a registrant's ability to record, process, summarize, and report" necessary filing information.[40]

In short, the guidance does not add any new reporting requirements, but rather treats cyber risks as ordinary business risks in adopting largely the same approach as current rules regarding material disclosure.[41] Furthermore, although the guidance provides information regarding disclosure requirements, it is not technically legally binding. In an introductory note, the guidance makes clear that it "is not a rule, regulation, or statement of the Securities and Exchange Commission."[42] However, the SEC's approach did

37 SEC, *supra* note 32.

38 *Id.*

39 *Id.*

40 *Id.*

41 Rodney F. Tonkovic, *An Overview of the SEC's Efforts to Construct a Regulatory Response to the Problem of Cybersecurity Issue No. 628,* CORP. GOVERNANCE GUIDE 10676407, WOLTERS KLUWER, May 30, 2014, 2014 WL 10676407.

42 SEC, *supra* note 32.

make it explicitly clear that companies must report cybersecurity risks under the same materiality standard as other disclosures, and failing to comply may result in SEC enforcement actions.

B. Bank Disclosure Requirements

Unlike the disclosure regime governing public companies, regulators have traditionally not subjected banks to the same materiality standard. Instead, regulators seek to maintain the confidentiality of bank financial information, due to banks' sensitivity to potential loss of investor and depositor confidence.[43] If banks are not publicly traded, they do not have to file any reports with the SEC but instead must disclose limited financial information with banking regulators such as the Federal Reserve and the Federal Deposit Insurance Corporation ("FDIC").[44]

In March 2005, several banking regulators decided that the danger of losing public confidence in banks was outweighed by growing cybersecurity threats.[45] In response, they promulgated the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.[46] This guideline includes an

[43] *See* Laurie Durcan & Bruce K. Riordan, *Banking Disclosures, Financial Privacy, and the Public Interest*, 6 ANN. REV. BANKING L. 391, 391 (1987).

[44] *Information About Some Companies Not Available from the SEC*, U.S. SEC. & EXCHANGE COMMISSION, https://www.sec.gov/answers/noinfo.htm [https://perma.cc/AC4H-NJD9] (last modified Nov. 26, 2013).

[45] *See generally* Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736 (Mar. 29, 2005).

[46] *See id.*; *see also* Heather Zachary & Nicole Ewart, *Cybersecurity, Privacy and Communications Webinar: Financial Privacy Primer*, WILMERHALE (Mar. 23, 2017), https://www.wilmerhale.com/uploadedFiles/Shared_Content/Events/Documents/2017-03-23-WilmerHale-webinar-financial-privacy-primer.pdf [https://perma.cc/T7ZA-D6U4]. The regulators involved in promulgating the regulation were the Office of the Comptroller of the Currency ("OCC"), the Treasury Department, the Board of Governors of the Federal Reserve System (the "Federal Reserve"), the

interpretation of the Gramm-Leach-Bliley Act requirement that banks maintain programs ensuring the security of customer information and protecting customer information against unauthorized access.[47] More importantly, the guidance prescribes a risk-based incident response program, including timely notification of customers affected by a breach.[48] The regulatory agencies clarify that the circumstances requiring notification are instances in which the bank has reason to believe that "misuse of its information about a customer has occurred or is reasonably possible."[49] The guidance also limits the type of information requiring notification to "sensitive customer information," defined as "a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account."[50]

In October 2016, following several high profile bank cyberattacks on targets like JPMorgan Chase[51] and Bangladesh's central bank,[52] several banking regulators

FDIC, and the Office of Thrift Supervision. Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736, 15,736 (Mar. 29, 2005).

47 *See* Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. at 15,751.

48 *Id.* at 15,743.

49 *Id.* at 15,749.

50 *Id.* at 15,745.

51 *See* Jessica Silver-Greenberg, Matthew Goldstein & Nicole Perlroth, *JPMorgan Chase Hacking Affects 76 Million Households*, N.Y. TIMES (Oct. 2, 2014, 12:50 PM), https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/ [https://perma.cc/HF25-DBAU].

52 *See* Raju Gopalakrishnan & Manuel Mogato, *Bangladesh Bank Official's Computer Was Hacked to Carry Out $81 Million Heist: Diplomat*, REUTERS (May 19, 2016, 1:07 AM), https://www.reuters.com/article/us-cyber-heist-philippines/bangladesh-bank-officials-computer-was-hacked-to-carry-out-81-million-heist-diplomat-idUSKCN0YA0CH [https://perma.cc/32GU-5KBV].

published an advance notice of proposed rulemaking for cyber-risk governance and management with stricter standards.[53] The proposed rule would require banks with fifty billion dollars or more in assets to develop and maintain a formal cyber-risk management strategy, implement cyber-risk assessment tests, and ensure that the organization's board of directors has adequate cyber expertise.[54] However, the proposed regulation is still in its embryonic stages and the three biggest financial industry groups have already lodged heavy criticisms that it is "impractical and technically infeasible."[55] Moreover, regulators under the Trump administration have recently signaled that they would not move forward with the proposed rule.[56]

---

[53] *See* Enhanced Cyber Risk Management Standards, 81 Fed. Reg. 74,315 (proposed Oct. 26, 2016). The notice was published by the Federal Reserve, the OCC, and the FDIC. *Id.*

[54] *See id.* at 74,320–25.

[55] *See* Email from Thomas M. Wagner, Managing Dir., Sec. Indus. & Fin. Mkts. Ass'n, Doug Johnson, Senior Vice President, Am. Bankers Ass'n & Richard Coffman, Gen. Counsel, Inst. of Int'l Bankers to Robert deV. Frierson, Sec'y, Bd. of the Fed. Reserve Sys., Legislative & Regulatory Activities Div., Office of the Comptroller of the Currency, & Robert E. Feldman, Exec. Sec'y, Comments, Fed. Deposit Ins. Corp. 3 (Feb. 17, 2017), https://www.sifma.org/wp-content/uploads/2017/05/SIFMA-ABA-and-IIB-Submit-Comments-to-Multiple-Agencies-on-Enhanced-Cyber-Risk-Management-Standards.pdf [https://perma.cc/LVC7-K7E3]; *see also* Paul Merrion, *Leading Financial Sector Groups Balk at Enhanced Cybersecurity Standards*, CQ ROLL CALL, Feb. 22, 2017, 2017 WL 693802. The letter criticizes the prescriptive nature of the requirements, and instead requests a risk-based approach. Wagner, et al., *supra*. More specifically, the letter underscores that the proposed "requirement of [a recovery time objective] of two hours for sector-critical systems is not technically feasible and might have the unintended consequence of restoring a system to operation before the nature of the threat or the effects of the event have been fully understood and remediated." *Id.* at 3.

[56] *See* Jody Westby, *Bon Appétit! Cyber Regs Are a Mouthful*, LEADER'S EDGE (Apr. 2018), https://leadersedgemagazine.com/articles/%202018/03/bon-appetit [https://perma.cc/N4T4-HSYH].

C. Federal Broker-Dealer Requirements

In contrast to both public companies and banks, broker-dealers have no current federal disclosure requirements to the public for cyber incidents. Similar to their treatment of banks, regulators have not traditionally subjected broker-dealers to the materiality disclosure standard of public companies or required them to make sweeping quarterly SEC filings.[57] Furthermore, broker-dealers were excluded from the interagency guidance in March 2005, which mandated banking disclosure requirements for cyber incidents.[58] In addition, the Financial Industry Regulatory Authority ("FINRA"), the primary self-regulator of the broker-dealer industry, has neither issued nor plans to issue any cybersecurity rules in the future.[59] However, FINRA did issue a report on cybersecurity best practices[60] and does independently review firms' compliance with SEC regulations.[61]

---

57 *See* Arthur B. Laby, *Reforming the Regulation of Broker-Dealers and Investment Advisers*, 65 BUS. LAW. 395, 402 (2010). Broker-dealers do, however, have some limited disclosure requirements regarding fair-dealing, conflicts of interest, credit terms, privacy policies, and sharing nonpublic customer information. *Guide to Broker-Dealer Registration*, U.S. SEC. & EXCHANGE COMMISSION, https://www.sec.gov/reportspubs/investor-publications/divisionsmarketregbdguidehtm.html [https://perma.cc/5PWK-84DQ] (last modified Dec. 12, 2016).

58 Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736, 15,738, n.6 (Mar. 29, 2005).

59 *A Few Minutes with FINRA: Cybersecurity – Part I*, FINRA (June 27, 2017), http://www.finra.org/industry/afmwf-cybersecurity-part1 [https://perma.cc/N8DN-NVMR] (showing an interview with Susan Axelrod, FINRA's Executive Vice President for the Office of Regulatory Operations, who explains that with regard to cybersecurity, FINRA's role is not to make rules but to "help firms understand where the issues and challenges are, help inform them of best practices, and continue to engage in where the firms individually can do better.").

60 FINRA, *supra* note 3.

61 *Cybersecurity*, FINRA, http://www.finra.org/industry/cybersecurity [https://perma.cc/737P-U9NP].

Although the SEC has not created a disclosure standard, it regulates broker-dealer cybersecurity through Regulations S-P and S-ID and enforces its guidelines through compliance examinations.[62] Furthermore, the Treasury Department requires that broker-dealers report suspicious activities, including cyberattacks, through regular filings.[63] Over the years, there have also been two unsuccessful attempts—through both legislative and regulatory means—to create a federal disclosure standard for broker-dealers.[64]

1. SEC Regulations S-P and S-ID

In June 2000, under congressional authorization from section 504 of the Gramm-Leach-Bliley Act of 1999, the SEC promulgated Regulation S-P to ensure that financial institutions protect the security and confidentiality of private consumer information.[65] The regulation prohibits broker-dealers and financial advisers from disclosing a customer's nonpublic personal information to nonaffiliated third-parties without first providing the customer a privacy notice and an opportunity to opt-out.[66] The regulation only addresses intentional disclosures made by the firm and does not require any disclosure to customers regarding unauthorized access to their information by third parties, such as computer hackers.

The regulation does, however, impose a duty on broker-dealers to adopt written policies and procedures designed to protect nonpublic personal customer information and prevent unauthorized intrusions.[67] These policies must ensure the security and confidentiality of customer

62 *See infra* Section II.C.1–2.

63 *See infra* Section II.C.3.

64 *See infra* Section II.C.4.

65 Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information, 17 C.F.R. § 248.1–100 (2018); *see also SEC Adopts Financial Privacy Rules*, INVESTMENT COMPANY INST. (June 29, 2000), https://www.ici.org/policy/regulation/privacy/00_SEC_PRIV_FINAL [https://perma.cc/E6WD-4PLC].

66 *See* 17 C.F.R. § 248.10 (2018).

67 *See id.* § 248.30.

information, protect against any foreseeable threats, and "[p]rotect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer."[68] To ensure compliance with this rule, the SEC issued another rule in 2003 requiring firms to "designate a chief compliance officer to be responsible for administering [the firm's] policies and procedures."[69]

As instructed by Congress after the financial crisis of 2008 in the Dodd Frank Act, the SEC and the Commodity Futures Trading Commission ("CFTC") jointly promulgated Regulation S-ID to prevent identity theft in "covered accounts."[70] The rule requires broker-dealers to establish written policies to "detect, prevent, and mitigate identity theft" using a red flags system that assesses potential risks to customer accounts.[71] Broker-dealers should authenticate the customers' identities, monitor transactions, and verify changes of customer addresses.[72] Firms should also be alert for warnings from consumer reporting agencies, unusual account activity, suspicious documents or personal information, and notices from customers or law enforcement about potential identity theft.[73]

---

68 *Id.*

69 Compliance Programs of Investment Companies and Investment Advisers, 68 Fed. Reg. 74,714, 74,714 (Dec. 24, 2003).

70 *See* Identity Theft Red Flags Rules, 78 Fed. Reg. 23,638, 23,640 (Apr. 19, 2013). The rule defines a "covered account" as "[a]n account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions" or "any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks." *Id.* at 23,644. The guidance specifically includes a brokerage account held with a broker-dealer in the definition. *Id.*

71 *Id.* at 23,640, 23,645–46.

72 *Id.* at 23,661.

73 *Id.*

Although not covered extensively, a footnote in the rule release mentions the risk of identity theft by cyber criminals who "con financial advisers into wiring cash out of their clients' online investment accounts" by tricking the adviser into legitimately executing a wire transfer so "cash flows into a bank account controlled by the thieves—leaving the victim in a dispute with the financial adviser over getting made whole."[74] While the rule instructs broker-dealers to prevent and detect these cyberattacks through risk assessment, it does not require any customer disclosures about cyberattacks, instead treating disclosure as one of several "appropriate" responses while investigating suspicious activity.[75]

2. SEC OCIE Examinations

The Office of Compliance Inspections and Examinations ("OCIE"), a branch of the SEC, was created in 1995 to conduct regular inspections of broker-dealers in order to protect investors and ensure market integrity.[76] OCIE monitors the behavior of market participants, improves firm compliance with SEC regulations and securities laws, and uses the results of its inspections to inform future SEC rule-making.[77] Recognizing the growing risk of cyberattacks to broker-dealers, OCIE launched a cybersecurity initiative in 2014 to assess broker-dealers' preparedness.[78] In its

---

[74] *Id.* at 23,642 n.57 (quoting Byron Acohido, *Cybercrooks Fool Financial Advisers to Steal from Clients*, USA TODAY (Aug. 26, 2012, 7:07 PM), http://usatoday30.usatoday.com/money/perfi/basics/story/2012-08-26/wire-transfer-fraud/57335540/1 [https://perma.cc/N69T-NLTR]).

[75] *See id.* at 23,661.

[76] *See* Lori A. Richards & John H. Walsh, *Compliance Inspections and Examinations by the Securities and Exchange Commission*, 52 BUS. LAW. 119, 119–20 (1996); *see also About the Office of Compliance Inspections and Examinations*, U.S. SEC. & EXCHANGE COMMISSION [hereinafter *About OCIE*], https://www.sec.gov/ocie/Article/ocie-about.html [https://perma.cc/8YDH-UYXL] (last modified July 21, 2017).

[77] *See About OCIE*, *supra* note 76.

[78] *See* Office of Compliance Inspections and Examinations, *OCIE Cybersecurity Initiative*, SEC NAT'L EXAM PROGRAM RISK ALERT, Apr. 15,

cybersecurity examination sweep, OCIE found that eighty-eight percent of the examined broker-dealers had been targeted by cyberattacks, while over half received fraudulent emails seeking to transfer client funds.[79] On the bright side, however, the overwhelming majority of broker-dealers examined had written information security policies and routinely conducted risk assessments to identify cybersecurity threats and vulnerabilities.[80] In other sweeps, OCIE focused on firm cybersecurity governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response.[81]

3. FinCEN SAR Reporting

Even though broker-dealers are not required to disclose cyberattacks to the public, they must report certain attacks to the government. Whenever a broker-dealer suspects a criminal violation or a transaction potentially involving money laundering exceeding specific monetary thresholds, it must file a Suspicious Activity Report ("SAR") with a Treasury Department bureau called the Financial Crimes Enforcement Network ("FinCEN").[82] In October 2016, FinCEN issued an advisory that financial institutions are required to report cyber events that involve $5000 or more in funds or assets.[83] Notably, FinCEN defines a cyber event as

2014, at 1, https://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf [https://perma.cc/YVB2-B92F].

79 *See* Office of Compliance Inspections and Examinations, *supra* note 2, at 2–3.

80 *See id.* at 2.

81 *See* Office of Compliance Inspections and Examinations, *OCIE's 2015 Cybersecurity Examination Initiative*, SEC NAT'L EXAM PROGRAM RISK ALERT, Sep. 15, 2015, at 2–3, https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf [https://perma.cc/4B3U-3X6U].

82 *See* 12 C.F.R. § 353.1–3 (2018).

83 *See* FIN. CRIMES ENF'T NETWORK, U.S. DEP'T OF THE TREASURY, FIN-2016-A005, ADVISORY TO FINANCIAL INSTITUTIONS ON CYBER-EVENTS AND CYBER-ENABLED CRIME 4 (2016) [hereinafter SAR ADVISORY], https://www.fincen.gov/sites/default/files/advisory/2016-10-

"[a]n attempt to compromise or gain unauthorized electronic access to electronic systems, services, resources, or information."[84] The bureau further clarifies that even unsuccessful hacking attempts must be reported.[85]

Since the purpose of an SAR is to help the government combat illegal activity, FinCEN encourages firms to report as much information about the cyber event as possible, including indicators of compromise, IP addresses, device identifiers, and the types of methodologies used.[86] Furthermore, FinCEN recommends that financial institutions pool resources and work together to identify potential threats and vulnerabilities.[87] However, firms must keep the existence of their reported SARs confidential to avoid tipping off the suspected criminals about law enforcement involvement.[88]

4. Unsuccessful Attempts at Disclosure Requirements

The federal government has unsuccessfully attempted to create a federal disclosure standard for broker-dealers regarding cyberattacks on various occasions. Since 2005, senators have introduced several pieces of legislation that would impose federal data breach notification requirements

25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf [https://perma.cc/Y6MF-Z245].

84 *Id.* at 1.

85 *See Frequently Asked Questions (FAQs) Regarding the Reporting of Cyber-Events, Cyber-Enabled Crime, and Cyber-Related Information Through Suspicious Activity Reports (SARs)*, FIN. CRIMES ENF'T NETWORK, (Oct. 25, 2016), https://www.fincen.gov/frequently-asked-questions-faqs-regarding-reporting-cyber-events-cyber-enabled-crime-and-cyber [https://perma.cc/T5DQ-KLHZ].

86 *See* SAR ADVISORY, *supra* note 83, at 6–7.

87 *See id.* at 8–9.

88 *See* 31 U.S.C. § 5318(g)(2) (2014); *id.* § 1020.320(e); FIN. CRIMES ENF'T NETWORK, FINCEN SUSPICIOUS ACTIVITY REPORT (FINCEN SAR) ELECTRONIC FILING INSTRUCTIONS (2012), https://www.fincen.gov/sites/default/files/shared/FinCEN%20SAR%20ElectronicFilingInstructions-%20Stand%20Alone%20doc.pdf [https://perma.cc/2BU7-6Z9K].

on businesses and federal agencies, but each failed. In June 2005, Senator Arlen Specter introduced the Personal Data Privacy and Security Act of 2005.[89] The bill mandated that

> any business entity or agency engaged in interstate commerce that involves collecting, accessing, using, transmitting, storing, or disposing of personally identifiable information shall notify, following the discovery of a security breach of its systems or databases in its possession or direct control when such security breach impacts sensitive personally identifiable information.[90]

Nearly identical bills were introduced in the Senate in 2007,[91] 2009,[92] 2011,[93] and 2014,[94] but none of these bills were passed by the Senate.[95] Moreover, a similar bill entitled the Data Security and Breach Notification Act was introduced to the Senate almost every year from 2010–2017.[96] In addition to requiring disclosure of breaches, this bill would impose a fine of at least $1000 and a prison sentence of up to five years for willfully concealing a

89 Personal Data Privacy and Security Act of 2005, S. 1332, 109th Cong. (2005).

90 *Id.*

91 Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. (2007).

92 Personal Data Privacy and Security Act of 2009, S. 1490, 111th Cong. (2009).

93 Personal Data Privacy and Security Act of 2011, S. 1151, 112th Cong. (2011).

94 Personal Data Privacy and Security Act of 2014, S. 1897, 113th Cong. (2014).

95 *See* Brett V. Newman, *Hacking the Current System: Congress' Attempt to Pass Data Security and Breach Notification Legislation*, U. ILL. J.L. TECH. & POL'Y 437, 449 (2015).

96 *See* Data Security and Breach Notification Act of 2010, S. 3742, 111th Cong. (2010); Data Security and Breach Notification Act of 2011, S. 1207, 112th Cong. (2011); Data Security and Breach Notification Act of 2012, S. 3333, 112th Cong. (2012); Data Security and Breach Notification Act of 2013, S. 1193, 113th Cong. (2013); Data Security and Breach Notification Act of 2014, S. 1976, 113th Cong. (2014); Data Security and Breach Notification Act of 2015, S. 177, 114th Cong. (2015); Data Security and Breach Notification Act, S. 2179, 115th Cong. (2017).

breach.[97] However, this bill was never passed by the Senate either.[98]

Alternatively, the SEC attempted to create a federal disclosure standard for businesses and federal agencies through a proposed amendment to Regulation S-P in 2008.[99] The proposed rule would transcend the general requirements of maintaining information security protocols and protecting customer information by adding specific steps that broker-dealers must take to prevent and respond to cyberattacks.[100] Firms would have to designate a specific employee to coordinate the security program, perform a written risk assessment, regularly test and monitor the effectiveness of the key controls against attacks and intrusions, routinely adjust the controls in light of testing, and provide training to employees about the information security protocols.[101]

The proposed rule would also require broker-dealers to establish procedures for responding to cyberattacks. Notably, firms must "promptly conduct a reasonable investigation and make a written determination of the likelihood that sensitive personal information has been or will be misused," and if misuse of the information has occurred or is reasonably likely, firms are required to "notify affected individuals as soon as possible."[102] Given that the notification is intended to prevent identity theft, the rule defines "sensitive personal information" as "any personal information, or any combination of components of personal information, that would allow an unauthorized person to use, log into, or access an individual's account, or to establish a new account

97 *See, e.g.*, Data Security and Breach Notification Act, S. 2179, 115th Cong. § 5(f) (2017).

98 *Current Legislation: All Information (Except Text) for S.2179 – Data Security and Breach Notification Act*, CONGRESS.GOV, https://www.congress.gov/bill/115th-congress/senate-bill/2179/all-info [https://perma.cc/6RZR-NBE4].

99 *See generally* Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information, 73 Fed. Reg. 13,692 (proposed Mar. 13, 2008).

100 *Id.* at 13,707–08.

101 *Id.* at 13,708, 13,713.

102 *Id*. at 13,713.

using the individual's identifying information."[103] If enacted, this disclosure standard would be nearly identical to the banking requirement imposed under the March 2005 Interagency Guidance.[104]

However, proposed rules are not legally binding until after they go through a public comment period, are modified, and are released as final rules.[105] Therefore, even though the amendment to Regulation S-P was proposed, considering the length of the time elapsed since proposal, it is highly unlikely that it will ever be promulgated as a final rule. Borrowing legislative terminology, the proposed regulation has suffered a fate equivalent to dying in committee. According to an internal audit of the SEC rulemaking process, for the twelve rules reviewed by the audit, the average time between the publication of proposed and final

103 *Id.* at 13,697. The proposed rule goes on to list specific pieces of information that would meet this definition, "including the individual's Social Security number, or any one of the individual's name, telephone number, street address, e-mail address, or online user name, in combination with any one of the individual's account number, credit or debit card number, driver's license number, credit card expiration date or security code, mother's maiden name, password, personal identification number, biometric authentication record, or other authenticating information." *Id.* at 13,697–98.

104 The March 2005 Interagency Guidance provides that "[w]hen a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible. Customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay. However, the institution should notify its customers as soon as notification will no longer interfere with the investigation." Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736, 15,752 (Mar. 29, 2005).

105 Rick Firestone & K.C. Goyer, *SEC Rulemaking and Implementation Under the Dodd-Frank Act*, WALLSTREETLAWYER.COM: SEC. ELECTRONIC AGE, Oct. 2010, 14 No. 10 GLWSLAW 14.

rules was 450 days.[106] In the past ten years of SEC data, the longest amount of time to finalize a proposed rule was just over three years.[107] Around a third of proposed rules are never acted upon and die in the rulemaking process.[108] Thus, given the nearly ten years of inaction, the proposed rule is moribund for all intents and purposes.

D. Emerging State Cybersecurity Regulations and Data Disclosure Requirements

1. State Cybersecurity Regulation

Over the past few years, several states—including New York, Colorado, and Vermont—have introduced regulations to address the growing threat of cyberattacks in the financial sector. In February 2017, the New York Department of Financial Services ("DFS") released regulations that require financial institutions operating in New York to develop a cybersecurity program, designate a Chief Information Security Officer, limit who has access to data or systems, notify the DFS of a cybersecurity event within seventy-two hours, and have a written incident response plan.[109]

In May 2017, Colorado adopted regulations that require broker-dealers operating in the state to establish procedures to ensure cybersecurity, including using secure email for confidential personal information, authenticating employee

106 The audit reviewed twelve rules from between 1999 and 2001. *See* SEC, RULEMAKING PROCESS, AUDIT NO. 347 (2002), https://www.sec.gov/oig/reportspubs/aboutoigaudit347finhtm.html [https://perma.cc/KZF6-UJ5G].

107 *Rulemaking Index*, U.S. SEC. & EXCHANGE COMMISSION, https://www.sec.gov/rules/rulemaking-index.shtml [https://perma.cc/EA8V-SFPR] (last modified Nov. 6, 2018).

108 From 2008–17, of the 141 unique rules that were proposed by the SEC, 93 of them became final rules and the other 48 did not. *Id.*

109 *See* N.Y. COMP. CODES R. & REGS. tit. 23, § 500 (2017); *see also* Daniel Ilan et al., *NYDFS Cybersecurity Regulations Take Effect*, CLEARY GOTTLIEB (Aug. 21, 2017), https://www.clearygottlieb.com/~/media/organize-archive/cgsh/files/2017/publications/alert-memos/nydfs-cybersecurity-regulations-take-effect-8-21-17.pdf [https://perma.cc/U6XB-4XKU].

access to sensitive information, and conducting routine risk assessments.[110] In May 2017, Vermont also promulgated cybersecurity regulations that require securities professionals operating in Vermont to establish information security protocols with nearly identical obligations to those in Colorado.[111] Although these regulations apply to broker-dealers operating in these states, they do not mandate any additional disclosure requirements.

2. Data Breach Notification Laws

Due to federal inaction, individual states have started enacting data breach notification laws for all entities doing business within their state; however, the laws vary greatly in their breadth and rigor.[112] California was the first state to pass a data breach notification law in 2002, but in the past two decades, all fifty states as well as the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted some form of data breach notification law.[113] This patchwork approach had resulted in inconsistent results, as when Target Corporation paid an $18.5 million settlement to forty-seven states in relation to its 2013 data breach, but Alabama was not included because it did not yet have a data breach notification law.[114] In other words, Target owed no legal obligation to Alabama residents to protect their

110 *See* COLO. CODE REGS. § 704-1:51-4.8 (2018).

111 *See* 4-4 VT. CODE R. § 8:8-4 (2018).

112 *See* Charlotte A. Tschider, *Experimenting with Privacy: Driving Efficiency Through a State-Informed Federal Data Breach Notification and Data Protection Law*, 18 TUL. J. TECH. & INTELL. PROP. 45, 63–65 (2015).

113 *Id.* at 63; *Security Breach Notification Laws*, NAT'L CONF. OF ST. LEGISLATURES (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/SK6P-Q82B]. Alabama and South Dakota, the last two states to do so, only passed such laws in 2018.

114 Leada Gore, *Why Alabama Isn't Cashing in on $18.5 Million Target Data Breach Settlement*, AL.COM (May 25, 2017), http://www.al.com/news/index.ssf/2017/05/why_alabama_isnt_cashing_in_on.html [https://perma.cc/UK3C-VTQQ].

personal information from hacking or to notify them about a breach.[115]

All state data breach notification statutes obligate entities to alert individuals when a data breach affects their personally identifiably information.[116] These laws, however, vary widely on what entities are covered, what constitutes "personally identifiably information," what type of notification must be provided, and whether data encryption provides a safe harbor.[117] For instance, individuals and government agencies must notify Alaskans by written or electronic means if their personal information is compromised during a breach, unless the information is encrypted and the encryption key remains secure.[118] Most states—including Alaska—define personally identifiably information to include names coupled with social security numbers, driver's license numbers, financial account or credit card numbers, or security codes or passwords that would allow access to the account.[119]

Thus, as one commentator put it, on a state level if "a [broker-dealer] experiences a breach, it is possible it could have no disclosures to make, or several, depending on where it is located and the nature of the information at issue."[120] However, the bare disclosure requirements mandated by states are insufficient. As discussed in greater detail below, the statutory definitions of personally identifiably information in state laws typically do not include many types of data that would be particularly sensitive to broker-dealer

115 *See id.*

116 *State Data Breach Laws Protected Personal Information Chart: Overview*, PRAC. L. INTELL. PROP. & TECH., 2015 WL 3938380 [hereinafter *State Data Laws*].

117 Tschider, *supra* note 112, at 65–71; *see also State Data Laws*, *supra* note 116.

118 *See* ALASKA STAT. ANN. § 45.48.010–090 (West 2018).

119 *See State Data Laws*, *supra* note 116; *see also* ALASKA STAT. ANN. § 45.48.090 (West 2018).

120 *See* Alan Wolper, *The Equifax Breach May Be a Problem for More than Just Equifax*, ULMER & BERNE (Sep. 28, 2017), https://www.bdlawcorner.com/2017/09/the-equifax-breach-may-be-a-problem-for-more-than-just-equifax/ [https://perma.cc/V79A-YC8Y].

customers, such as transactional information and trade histories.[121]

E. European Union's General Data Protection Regulation

Unlike the United States' patchwork of state and federal regulations (with industry-specific variations), the European Union recently overhauled its cybersecurity regime with the General Data Protection Regulation ("GDPR").[122] Before the GDPR, the European Union regime mirrored that of the United States, governed piecemeal by conventions, directives, treaties, and individual European country rules.[123] With the GDPR now in effect, however, there is a greater degree of uniformity.[124]

The GDPR requires all organizations to implement technical measures to safeguard personal information, conduct risk assessments, and restrict usage of third party processors to those in compliance with the GDPR's standards.[125] Furthermore, the GDPR sets forth a universal

121 *See infra* Section III.B.

122 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR]. *See generally* Christina Glon, *Data Protection in the European Union: A Closer Look at the Current Patchwork of Data Protection Laws and the Proposed Reform That Could Replace Them All*, 42 INT'L J. LEGAL INFO. 471, 472 (2014).

123 Glon, *supra* note 122, at 472.

124 The GDPR went into effect on May 25, 2018. Jeewon Kim Serrato, Marcus Evans, Ffion Flockhart & Steven Hadwin, *One Week into GDPR – What You Need to Know*, NORTON ROSE FULBRIGHT (June 4, 2018), https://www.dataprotectionreport.com/2018/06/one-week-into-gdpr-what-you-need-to-know/ [https://perma.cc/9878-85B6]; *see also* Courtney M. Bowman, *A Primer on the GDPR: What You Need to Know*, PROSKAUER ROSE (Dec. 23, 2015), https://privacylaw.proskauer.com/2015/12/articles/european-union/a-primer-on-the-gdpr-what-you-need-to-know/ [https://perma.cc/J39Q-6TEM].

125 Colin Pearson et al., *Cybersecurity in the EU – The New Regime Under the GDPR and NISD*, CLEARY GOTTLIEB (May 3, 2017), https://www.clearygottlieb.com/~/media/organize-

data breach notification requirement: when a "personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay" in clear and plain language, unless the information is encrypted and inaccessible to the unauthorized user.[126] However, both the encryption safe haven and the demanding threshold of "high risk to the rights and freedoms" lessen the burden of the universal requirement.

III. SPECIFIC BROKER-DEALER DISCLOURE CONCERNS

A. Effects of Broker-Dealer Disclosures

The need for a broker-dealer disclosure requirement is different from that of a public company, given the unique role played by broker-dealers in the financial markets. Broker-dealers buy and sell securities, acting as agents when they execute orders on behalf of their clients and as dealers when they trade on their own account.[127] They are the primary interface between investors and the market, and they ensure the free flow of securities.[128] Yet, without the listed stock prices available for public companies, their actions are not subject to any form of information discipline mechanism to hold them accountable to their investors.[129]

archive/cgsh/files/publication-pdfs/alert-memos/2017/cybersecurity-in-the-eu—the-new-regime-under-the-gdpr-and-nisd-5-5-17.pdf [https://perma.cc/ZS8A-MHYJ].

126 GDPR at art. 34, 2016 O.J. (L 119) 1.

127 *Broker-Dealer*, INVESTOPEDIA, https://www.investopedia.com/terms/b/broker-dealer.asp [https://perma.cc/5W36-HSRX].

128 *Id.*

129 *See Staff Guidance for Filing Broker-Dealer Notices, Statements, and Reports*, U.S. SEC. & EXCHANGE COMMISSION, https://www.sec.gov/divisions/marketreg/bdnotices.htm [https://perma.cc/7PS6-K32U] (last modified May 24, 2017) (underscoring that most broker-dealer disclosures are provided to their designated examining authority, not to consumers). Broker-dealers must disclose to customers their certified balance sheet and information relating to their

Thus, the purpose of cybersecurity disclosures in a broker-dealer context is not to provide better information to investors about their investments. Instead, it functions to alert them about the safety and security of their investments as a whole and to incentivize the broker-dealer to institute better security policies.[130] A notification from a broker-dealer would signal the severity of the situation to the customer.

Given the lack of information discipline mechanisms and public oversight, there is reason to consider disclosure a bare minimum requirement. There may even be justification for using a strict scrutiny standard or imposing an affirmative duty of care to safeguard against the threat of attacks. However, the specifics and potential risks of any new affirmative duty are beyond the scope of this Note.

It is also important to consider that security concerns, not privacy concerns, form the basis of the current regulatory regime for broker-dealers.[131] SEC Regulations S-P and S-ID target organizational practices such as establishing security protocols and monitoring for suspicious account activity.[132] These regulations focus on breach prevention, rather than addressing the resultant *consequences* of a breach. In effect, this security-oriented framework is missing an emphasis on the concrete harms a breach inflicts upon individuals.[133] Thus, a proposed disclosure requirement must balance organizational constraints with the potential damage to individuals from their lack of notification.

B. Sensitive Information Collected by Broker-Dealers

Broker-dealers are also unique in the types of information they acquire from customers. The range of data broker-dealers collect extends beyond social security numbers and

financial condition, but there is no pricing mechanism affected by these disclosures, as in public companies. *See* 15 U.S.C. § 78q(e)(1)(B) (2012).

130 *See* Priscilla M. Regan, *Federal Security Breach Notifications: Politics and Approaches*, 24 BERKELEY TECH. L.J. 1103, 1113 (2009).

131 *See id.* at 1114.

132 *See supra* Section II.C.1.

133 Regan, *supra* note 130, at 1114.

credit card information, but state breach notification laws do not adequately address this broader scope.[134] In 2003, the Treasury Department and several regulatory agencies jointly issued a rule mandating that broker-dealers must establish and maintain a customer identification program.[135] Among other provisions, the rule requires that when a customer opens up a new account with a broker-dealer, the firm must collect and verify their name, date of birth, address, and social security number.[136] These types of information are largely covered by the patchwork of state laws, but other information—including data collected in response to FINRA's Know Your Customer Rule and Suitability Rule—are not addressed by any disclosure regime. Yet, if breached, they may have consequences just as dire.

Under the Know Your Customer Rule, broker-dealers must "use reasonable diligence, in regard to the opening and maintenance of every account, to know. . . the essential facts concerning every customer" and which individuals are authorized to act on behalf of such customer.[137] The Suitability Rule goes even further, requiring firms to "have a reasonable basis to believe that a recommended transaction or investment strategy involving a security. . . is suitable for the customer."[138] The rule requires firms to base their investment strategy decisions on the customer's investment profile, including "the customer's age, other investments, financial situation and needs, tax status, investment objectives, investment experience, investment time horizon, liquidity needs, risk tolerance," and other relevant

134 *See infra* text accompanying notes 137–139.

135 *See* Customer Identification Programs for Broker-Dealers, 68 Fed. Reg. 25,113, 25,113 (May 9, 2003).

136 *See* 31 C.F.R. § 1023.220 (2018). Although this rule only applies to individuals opening up accounts (as opposed to entities), FinCEN recently enacted a rule that requires that the same information be collected about certain officers and owners of any entity opening an account. *See* Customer Due Diligence Requirements for Financial Institutions, 81 Fed. Reg. 29,398 (May 11, 2016).

137 FINRA, Rule 2090 (2012).

138 FINRA, Rule 2111 (2014).

information that the customer provides.[139] Furthermore, as the agent buying and selling securities for a customer, a broker-dealer has access to a customer's transaction information and trading history.

If a cyberattack compromises any of these types of information, including an investor's investment history and risk tolerance, the consequences could potentially be devastating. For instance, an investor may face backlash from friends and the public at large for investments in companies that contravene the investor's public political leanings. We can analogize to recent consumer backlashes regarding public companies that made political contributions to particular candidates or political parties.[140] In a similar vein, if it became public that an individual invests in companies with poor environmental records or those utilizing child labor, it could greatly harm the individual's reputation and finances.

Moreover, a high net worth investor or hedge fund may have a proprietary investing strategy that would lose its value if revealed to the public. In 2015, security companies Kroll and FireEye investigated several incidents involving hackers who stole secret algorithms and trading tactics.[141] Some analysts consider such a cybersecurity threat even more concerning than a market crash, given that "[c]omputer source codes and proprietary trading methods are often the lifeblood of a company's business model."[142] Although not

139 *Id.*

140 For instance, in August 2018, In-N-Out Burger faced social media calls for a boycott after it was revealed that the fast food chain had donated $25,000 to the California Republican Party. *See* Jeff Daniels, *In-N-Out Burger's $25,000 Donation to California GOP Brings Call for Boycott from Democrats,* CNBC (Aug. 30, 2018), https://www.cnbc.com/2018/08/30/in-n-out-burger-faces-boycott-for-california-gop-donation.html [https://perma.cc/987X-MB6A].

141 *See* Mathew J. Schwartz, *Hackers Steal Trading Algorithms*, BANKINFOSECURITY (Feb. 26, 2015), https://www.bankinfosecurity.com/hackers-target-trading-algorithms-a-7949 [https://perma.cc/TE43-BKFS].

142 *See id.*; *see also* Kip McDaniel, *Hacking a Hedge Fund*, CHIEF INV. OFFICER (Nov. 20, 2015), https://www.ai-cio.com/news/hacking-a-hedge-fund/ [https://perma.cc/4DVK-49YR].

addressed by state disclosure laws, a privacy-focused disclosure requirement geared towards broker-dealers would require that breaches of these categories of sensitive and proprietary information trigger notification to customers. This approach would provide customers with advance notice and a chance to perform damage control before the information potentially became public.

C. Materiality Standard

The public company materiality standard—requiring disclosures based on the likelihood that a reasonable investor would find the information important for an investment decision—is inapposite for broker-dealers, given the lack of information discipline mechanism and lack of public oversight.[143] Additionally, state data breach disclosure laws do not provide any uniform guidelines. In some states, firms have a duty "to notify about any breach of security, while other states require notification of breach only when there is a reasonable likelihood of harm."[144] Since Massachusetts is arguably the state with the strictest data disclosure laws, one commentator suggested that companies should follow Massachusetts rules as a convenient and cost-saving rule of thumb.[145] Yet this advice is not as easy to follow as it seems, given differences in state laws regarding how information must be reported (i.e. whether only reporting to individuals, or also to state enforcement and credit agencies) and what information such reports must include.[146]

It is important to note that, even if disclosure obligations are expanded to address broker-dealer specific concerns, one cannot abandon the materiality standard in a broker-dealer

143 *See supra* Section III.A.

144 *See RSA 2012: Getting Strict with State Data Breach Notification Laws*, INFOSECURITY MAG. (Feb. 29, 2012) [hereinafter *RSA 2012*], https://www.infosecurity-magazine.com/news/rsa-2012-getting-strict-with-state-data-breach/ [https://perma.cc/LQU5-S27J].

145 *See id.*

146 *See id.*

context. A threshold for triggering disclosure is justified by the same rationale for broker-dealers as for public companies. If broker-dealers were required to report even immaterial events, consumers would be bombarded by an avalanche of notifications, which "can cause either undue alarm or desensitization to events of true concern."[147]

However, one key difference in application of a new disclosure regime for broker-dealers would be the emphasis of the threshold. To address cybersecurity concerns, the triggering threshold must consider the privacy-oriented nature of disclosures. For example, the GDPR in the European Union takes such a perspective. The trigger requiring GDPR disclosure is when there is a personal data breach unless it is "unlikely to result in a high risk to the rights and freedoms of natural persons."[148] Despite the change in focus, though, this is a very high threshold and may not be inclusive enough to address the needs of broker-dealer customers, as discussed above.[149] In adopting a broker-dealer specific standard, regulators could tweak this threshold to require disclosure "when the personal data breach is likely to result in substantial financial or reputational costs to customers." This adjustment would protect broker-dealer customers against identity theft and loss of funds, and obligate broker-dealers to warn clients in the event that other sensitive information is accessed.

Firms would be misguided to treat all threats equally when making determinations about resource allocation. A more compelling framework would construct a privacy threat continuum, with responses required in proportion to each threat. Consider a typical financial firm that uses a multilayered security approach including firewalls, antivirus software, spam filters, authentication, account monitoring,

147 *See* Loren F. Selznick & Carolyn LaMacchia, *Cybersecurity: Should the SEC Be Sticking Its Nose Under This Tent?*, 2016 U. ILL. J.L. TECH. & POL'Y, 35, 52 (2016).

148 GDPR at art. 33, 2016 O.J. (L 119) 1.

149 *See supra* Section II.E.

encryption, and offsite data backup.[150] Different types of threats—such as web application attacks, distributed denial of service ("DDoS") attacks, data breaches, and insider attacks—may compromise different types of information.[151] Companies would also be wise to protect their most sensitive information with the highest level of security, further justifying a continuum framework.[152]

On one end of the spectrum, a simple DDoS attack that brings down a company's website may alarm the company about the need for better defenses, but if databases with customer information are never threatened, there would be no need to alert customers. Arguably, alerting customers would be detrimental, since such a notification would desensitize them to more serious threats.[153] On the other end of the spectrum, a data breach by a hacker or an insider could compromise actual financial funds or key identifying information usable to steal a customer's identity. In such a case, the broker-dealer should immediately alert customers and help them take preventative action, like alerting the three credit bureaus and encouraging customers to monitor and freeze their credit.[154] In addition, while a broker-dealer's suitability database is typically not covered by disclosure laws, if it is compromised and information about customer investing habits falls into the hands of a hacker, the firms

150 *See How Multi-Layered Network Protection Works*, SOLARWINDS MSP, https://www.solarwindsmsp.com/content/multi-layered-security-approach [https://perma.cc/5Y25-M48X].

151 *See Top 4 Cyber Threats Facing the Financial Services Industry*, IMPERVA (July 18, 2016), https://www.imperva.com/blog/2016/07/top-4-cyber-threats-facing-the-financial-services-industry/ [https://perma.cc/5XEJ-D57A].

152 *See* Jans Aasman, *Triple Attributes: A New Way to Protect the Most Sensitive Information*, DATACONOMY (Oct. 4, 2017), http://dataconomy.com/2017/10/triple-attributes-new-way-protect-sensitive-information/ [https://perma.cc/75RM-U2AG].

153 *See* Selznick & LaMacchia, *supra* note 147, at 52.

154 *See* Ron Lieber, *How to Protect Yourself After the Equifax Breach*, N.Y. TIMES (Oct. 16, 2017), https://www.nytimes.com/interactive/2017/your-money/equifax-data-breach-credit.html [https://perma.cc/87YM-GU53].

should alert customers. However, in this scenario, the disclosure should not require as much urgency and detail, given that the information does not directly compromise financial information.

One further complicating factor is that a broker-dealer may not know that it suffered a cyberattack.[155] Alternatively, even if it is aware that a hacker breached its databases, it may not know exactly what information was stolen.[156] Under those circumstances, the duty to disclose should attach at the time when the company discovers the extent of the attack.

Similar to public companies' disclosures, broker-dealers' disclosures should not only be reactive, they should also be proactive, informing customers about the risks of a potential breach. Although the threshold cannot be the same as the standard applied to a public company (i.e., whether the security issues are among the most significant factors making the investment risky), broker-dealers should inform customers if there is a high probability that sensitive customer information is at risk. Such a determination would necessarily hinge upon subjective factors, such as the currency of a broker-dealer's software patches, the broker-dealer's safety protocols compared to industry standards, prior cyberattack attempts, and internal employee issues.[157]

---

155 *See* Matthew F. Ferraro, Note, *"Groundbreaking" or Broken? An Analysis of SEC Cybersecurity Disclosure Guidance, Its Effectiveness, and Implications*, 77 ALB. L. REV. 297, 310 (2014).

156 *See* Mark Jewell, *T.J. Maxx Theft Believed Largest Hack Ever*, NBC NEWS (Mar. 30, 2007, 11:17 AM), http://www.nbcnews.com/id/17871485/ns/technology_and_science-security/t/tj-maxx-theft-believed-largest-hack-ever/ [https://perma.cc/8UPN-3ZBB] (illustrating how when T.J. Maxx was hacked, although it knew about the breach, it took longer to discover exactly what information was compromised).

157 The National Institute for Standards and Technology implemented the Framework for Improving Critical Infrastructure Cybersecurity in 2014, later amended in 2017, to provide private sector firms with guidance on improving their cybersecurity standards. This framework can be used by broker-dealers as one tool to assess the adequacy of their security controls. *See* NAT'L INST. STANDARDS & TECH., U.S. DEP'T COMMERCE, *NIST Releases Update to Cybersecurity Framework*, NIST (Jan. 10, 2017),

Furthermore, as is standard practice under many state disclosure requirements, the new standard should include a safe harbor for successful encryption.[158] If hackers or insiders obtain access to raw encrypted data but lack the encryption key to view the underlying information, there is no need to issue a disclosure to customers. This safe harbor for successful encryption will ensure a proper materiality standard and also encourage firms to maintain strong encryption systems.

D. Level of Detail in a Mandated Disclosure

When disclosing information that meets the materiality threshold, broker-dealers must still consider how much information must be disclosed. In the corporate context, mandatory disclosures can lower agency costs by compelling a corporation's directors to take better account of the shareholders' interests.[159] Similarly, providing broker-dealer customers with an adequate assessment of cyber risks can help consumers decide whether to open an account and, if so, with which firm, while also incentivizing firms to bolster their security controls. Failing to do so may result in embarrassing disclosures to their customers and consequent reputation costs.

Nevertheless, broker-dealers that fall prey to cyberattacks may not want to disclose too much information, as over-disclosure could reveal their security weaknesses and allow other hackers to exploit them, attack them again, or attack similarly situated broker-dealers.[160] For instance, with access to technical information about a firm, hackers can construct a "spear-phishing" attack using social

https://www.nist.gov/news-events/news/2017/01/nist-releases-update-cybersecurity-framework [https://perma.cc/PXV9-8W6V].

158 *See supra* Section II.D.2.

159 *See generally* Paul G. Mahoney, *Mandatory Disclosure as a Solution to Agency Problems*, 62 U. CHI. L. REV. 1047, 1048 (1995) (arguing "that the principal purpose of mandatory disclosure is to address certain agency problems that arise between corporate promoters and investors, and between corporate managers and shareholders").

160 *See* Ferraro, *supra* note 155, at 310.

engineering strategies, like posing as an employee or vendor of the firm in order to access critical parts of the firm's security technology infrastructure.[161] In effect, when deciding the level of specificity for a mandated disclosure, firms must consider an important tradeoff between ex-ante deterrence and ex-post revelation of damaging information to potential hackers.[162]

Therefore, regulators should consider a bifurcated approach to disclosure requirements. For actual data breaches, the balance should tip towards a much greater level of specificity. Customers should have the right to know exactly what type of information was stolen, as this will inform any precautionary measures they take in response. On the other hand, for disclosure of potential risks, the broker-dealer should communicate to customers in generalities, without enough technical information to tip off potential hackers. Despite the unspecific disclosures, customers should feel secure knowing that regulators have more direct access and information, in the form of SARs and occasional OCIE examinations.[163]

Alternatively, in the corporate arena, some commentators have suggested novel approaches that may provide even more assurance to customers. For instance, firms can voluntarily subject themselves to an audit by an independent cybersecurity auditor, who would review their security protocols and issue a public grade.[164] One might analogize such a system to New York City's restaurant health rating, simplifying a complex set of metrics into an easily understandable letter grade.[165] This would provide the assurance of a detailed disclosure without the risks

161 *See* Selznick& LaMacchia, *supra* note 147, at 58.

162 *See id.* at 63–64.

163 *See supra* Section II.C.2–3.

164 Selznick & LaMacchia, *supra* note 147, at 61.

165 *See, e.g.*, Jonathan Wolfe, *New York Today: What Do Restaurant Grades Mean?*, N.Y. TIMES (May 17, 2017), https://www.nytimes.com/2017/05/17/nyregion/new-york-today-what-do-restaurant-grades-mean.html [https://perma.cc/XSC7-9P8T].

associated with revealing technical information.[166] However, it is not clear how many firms would voluntarily subject themselves to such an audit, or if regulators would be willing to impose a mandatory audit system.

E. Cost to Smaller Broker-Dealers

As with any new regulation, regulators must consider the burden imposed by additional disclosure requirements on small and midsized broker-dealers that lack the resources and staffing available to larger firms. Full compliance with new regulations would often require firms to make large investments in technology or staffing, costs that might far exceed their budgetary constraints.[167] For this reason, small firms rarely make it through FINRA exams or SEC audits without being subjected to fines for regulatory infractions.[168] In fact, some analysts partially attribute the sharp decline in registered broker-dealers over the past decade to a large increase in regulations that disproportionately impact small firms and overwhelm their compliance departments.[169]

Regulators can mitigate the burdens of new regulations on small firms by providing exemptions for firms based on revenues or number of employees. Nevertheless, it is not

166 *See* Selznick & LaMacchia, *supra* note 147, at 68.

167 *See* Bruce Kelly, *2017 to Be Year of Independent Broker-Dealer Mergers*, INVESTMENT NEWS (Jan. 22, 2017), http://www.investmentnews.com/article/20170122/FREE/170119915/2017-to-be-year-of-independent-broker-dealer-mergers [https://perma.cc/L8SX-FCJC] (discussing the budgetary and revenue concerns facing smaller broker-dealers).

168 *See* Ross David Carmel, *The DOL Fiduciary Rule's Effect on Small Broker-Dealers*, INVESTMENT NEWS (May 4, 2016), http://www.investmentnews.com/article/20160504/BLOG09/160509969/the-dol-fiduciary-rules-effect-on-small-broker-dealers [https://perma.cc/KBA9-D9BV].

169 *See* Hester Peirce, *Dwindling Numbers in the Financial Industry*, BROOKINGS (May 15, 2017), https://www.brookings.edu/research/dwindling-numbers-in-the-financial-industry/ [https://perma.cc/2NK7-88VF]. The number of registered broker-dealers declined from 5892 in March 2007 to 3989 in March 2017, a timeframe during which there was also a sharp increase in CFTC and SEC regulations. *Id.*

clear how much of a burden a disclosure requirement would impose. Under financial responsibility rules, firms must already have the resources to send out limited financial disclosures to customers on a regular basis.[170] Furthermore, even if there are unintended burdens that would disproportionately impact smaller firms, regulators should impose the requirement under Calabresi and Hirschoff's economic principle of "cheapest cost avoider."[171] As between the firm and its customers, the firm has the greater ability to protect sensitive customer information from data breaches and should therefore bear both the financial liability and responsibility of notifying customers about a data breach. Moreover, as discussed further below, a federal disclosure standard for broker-dealers may actually end up saving costs for smaller firms by removing duplication and inconsistencies in the current patchwork system of state regulations.[172]

IV. POLICY RECOMMENDATIONS

A. Congress vs. SEC

Congress and the SEC are the two potential entities that may be tasked with imposing a new broker-dealer cybersecurity disclosure standard. As proposed by individual Senators numerous times, Congress may enact a sweeping disclosure bill to tidy up all of the gaps in the current state system.[173] Alternatively, under authorization from Congress in the Securities Exchange Act of 1934, the SEC may promulgate a new rule aimed at broker-dealers.[174]

170 *See* 15 U.S.C. § 78q(e)(1)(B) (2012).

171 *See generally* Guido Calabresi & Jon T. Hirschoff, *Toward a Test for Strict Liability in Torts*, 81 YALE L.J. 1055 (1972) (explaining the concept of a cheapest cost avoider).

172 *See infra* Section IV.B.

173 *See supra* Section II.C.4.

174 *See* Norah C. Avellan, Note, *The Securities and Exchange Commission and the Growing Need for Cybersecurity in Modern Corporate America*, 54 WASHBURN L.J. 193, 216–26 (2014). *See generally* Joyce Shulman-Kanciper, *The* Basic *Rules of Disclosure*, 62 ST. JOHN'S L. REV.

The current political climate is the primary obstacle to congressional legislation. As partisan discord and political gridlock continue in Washington, it is much harder for Congress to take on any comprehensive reform initiative, much less one that could anger business lobbyists.[175] Even proposals with bipartisan backing—like the Personal Data Protection and Breach Accountability Act of 2014, proposed by Senator Richard Blumenthal, and the Personal Data Notification & Protection Act of 2015, proposed by President Barack Obama—lacked the support necessary for passage.[176] Unless a compelling external impetus arises, such as a crippling financial cyberattack, it is unlikely that Congress will use its political capital to enact new financial disclosure obligations.

Another obstacle to congressional legislation is that a statute would be a blunt instrument in a situation that requires fine tuning. Both of the bill proposals mentioned above address cybersecurity disclosures in the financial system as a whole, without singling out specific segments.[177] Congress does not have the institutional competence to iron out disclosure requirements for each segment of the financial system.

In contrast, the SEC operates more independently from political pressure, with staggered five-year commissioner terms and organizational representation from both political parties.[178] Although the SEC may face pushback and should take into account valid industry concerns expressed during

704 (1988) (discussing the SEC's enforcement powers under the Securities Exchange Act of 1934).

175 *See* Aaron Blake, *Gridlock in Congress? It's Probably Even Worse than You Think*, WASH. POST (May 29, 2014), https://www.washingtonpost.com/news/the-fix/wp/2014/05/29/gridlock-in-congress-its-probably-even-worse-than-you-think/?utm_term=.8df16ef51e97 [https://perma.cc/MJ98-DKU8].

176 *See* Newman, *supra* note 95, at 451–55.

177 *Id.* at 453–455.

178 *See* Gary Shorter, *Introduction to Financial Services: The Securities and Exchange Commission (SEC)*, CONG. RES. SERV. (Jan. 9, 2017), https://fas.org/sgp/crs/misc/IF10032.pdf [https://perma.cc/9WUK-46JL].

the proposed rule's comment period, the SEC is neither elected by nor directly politically accountable to the industry.[179] This provides the SEC with much greater latitude to balance important consumer interests with broker-dealer constraints.

Further, the SEC has already proved itself adept at tailoring disclosure requirements for both public companies and the banking industry.[180] The SEC previously contemplated a new broker-dealer disclosure requirement in the proposed amendment to Regulation S-P in 2008.[181] Finally, with the growing threats to cybersecurity, the SEC will likely have more political support than it did a decade ago. For all of these reasons, the SEC—as opposed to Congress— should take up this issue.

B. Federal Preemption

Similar to what the European Union realized before it enacted the GDPR, our current patchwork system of state disclosure laws in the United States is a regulatory nightmare, especially for smaller broker-dealers.[182] State laws differ on what materiality threshold triggers a disclosure. Some require disclosure only for an actual breach, while others require disclosure even if there is just a reasonable likelihood of harm.[183] Moreover, even if a disclosure is triggered, states have different procedures for the necessary methods and recipients of a disclosure.[184]

Under the current system, firms must understand all the subtleties of the various state laws, develop them into different disclosure systems in practice, and keep track of

179 *See* Firestone & Goyer, *supra* note 105.

180 *See supra* Section II.A–B.

181 *See supra* Section II.C.4.

182 *See* Jacqueline May Tom, *A Simple Compromise: The Need for a Federal Data Breach Notification Law*, 84 ST. JOHN'S L. REV. 1569, 1570 (2010).

183 *See RSA 2012*, *supra* note 144.

184 *See id.*

any new amendments to state laws.[185] Therefore, like the GDPR, any new disclosure system for broker-dealers must preempt all of the existing state laws.[186] Far from only serving to benefit consumers, preemption will cut a great deal of the regulatory red tape and reduce resources devoted to following changes in individual state disclosure laws.[187]

One potential issue with federal field preemption is that any states that currently have stricter laws—Massachusetts, for instance—could end up with losses in protection for their residents.[188] Moreover, if there are new technological developments, states will have their hands tied behind their backs in trying to protect their citizens from threats and will have to wait for federal regulators to catch up. However, the SEC regularly amends old rules to reflect changing practices and technological advancements, and can act again if the need arises. Furthermore, instituting a baseline system offering protection for everyone is better than some individuals lacking any protections at all.

C. New Guidelines

Under the privacy-oriented framework laid out above, the new federal broker-dealer cybersecurity disclosure regulations must take into account an appropriate materiality standard, the types of information relevant to ordinary broker-dealers, and a tailored level of detail in the disclosure.[189] Given the sheer amount of data that broker-dealers collect to comply with the Know Your Customer Rule and the Suitability Rule, the information protected by a disclosure should transcend ordinary bank account and social security information.[190] In order to maintain public confidence in the broker-dealer system, the new regulation should also protect information with reputational or privacy

185 *See* Tom, *supra* note 182, at 1570.

186 *Id.* at 1589–94.

187 *Id.* at 1590.

188 *Id.* at 1589–90.

189 *See supra* Part III.

190 *See supra* Section III.B.

considerations to clients, including trading history, investment objectives, and risk tolerance.[191]

To that end, the requisite materiality standard that triggers a disclosure should be "when the personal data breach is likely to result in substantial financial or reputational costs to customers."[192] This threshold would take into account existing identity theft and embezzlement concerns, but would also include a more expansive view of client privacy concerns.[193] Furthermore, to facilitate appropriate resource allocation, this standard would allow broker-dealers to respond in proportion to the threat, based on a privacy spectrum. Whereas simple DDoS attacks would not warrant any disclosure, compromised reputational information would require moderate disclosure, and compromised financial information would require timely and extensive disclosure.[194]

When considering the level of detail to disclose, broker-dealers should be wary of accidentally aiding future hackers with overly specific technical information.[195] Whereas broker-dealers report SARs to FinCEN in abundant detail, disclosures to clients should address technical security information in broad generalities; specificity should be focused on details about the customer information breached and what steps the client can take to prevent any further harm.[196] Finally, although smaller broker-dealers may criticize the new regulation as overly burdensome, there should not be any exemptions based on revenues or number of employees.[197] The only way to fully protect broker-dealer customers is through uniform and consistent policies, and smaller firms will enjoy the benefits of federal preemption,

191 *See supra* Section III.B.

192 *See supra* Section III.C.

193 *See supra* Section III.C.

194 *See supra* Section III.C.

195 *See supra* Section III.D.

196 *See supra* Section III.D.

197 *See supra* Section III.E.

which should cause a net decrease to their compliance expenditures.[198]

V. CONCLUSION

In the current financial regulatory system, public companies and banks must disclose to consumers cyberattacks that affect their sensitive personal information. However, broker-dealers are noticeably absent from the equation, after both Congress and the SEC failed in attempts to introduce new requirements. The SEC should look to recent developments in the European Union and individual states that have pioneered data disclosure notification rules and adopt a broad cybersecurity disclosure requirement for broker-dealers. The disclosure would inform anyone who has a brokerage account if their information has been hacked and what the potential risks of maintaining a brokerage account are vis-à-vis cybersecurity.

One major departure from prior standards would be a focus on consumer privacy, as opposed to firm security, which is already comprehensively addressed in the regulatory sphere. Within this model, personal information would include more than just credit card and social security numbers, and would even encompass sensitive information about trading habits and investor profiles. The disclosure requirement would follow a spectrum, in proportion to the importance of the information at risk and the potential consequences for consumers. Moreover, to protect the interests of broker-dealers more broadly, federal preemption of state laws would remove some of the current hassles of complying with disclosure regulations, especially for smaller firms.

198 *See supra* Section III.E.