Nebraska Law Review

Volume 96 | Issue 2 Article 9

2017

The SEC's Data Dilemma: Addressing a Modern Problem by Encouraging Innovation, Responsibility, and Fairness

Gregg Moran
University of Nebraska College of Law

Comment*

The SEC's Data Dilemma: Addressing a Modern Problem by Encouraging Innovation, Responsibility, and Fairness

TABLE OF CONTENTS

* Gregg Moran, J.D. candidate, University of Nebraska College of Law.

I'd like to thank my family and friends for their support, especially my wife, Julianna (whose never-ending ability to put up with my nonsense ought to be grounds for canonization someday). I'd also like to thank all my professors at the College of Law, including Professor Joel Bacon, Professor Jack Beard, and Professor Justin (Gus) Hurwitz. Special thanks goes to Professor C. Steven Bradford. Finally, thank you to the members of the Nebraska Law Review, including this Comment's wonderful executive editor, Lora Waeckerle. All typos, errors, and bad opinions are my own.

I. INTRODUCTION

It was the story of every investor's nightmares. In late 2014, investment bank Morgan Stanley discovered a data breach—one that potentially compromised private information from hundreds of thousands of customer accounts—during a routine sweep.[1] Although Morgan Stanley had taken precautions against outside attackers, its defenses had a major weak point: threats from within the company. An employee of Morgan Stanley had exploited a security weakness in Morgan Stanley's employee server and taken the data in an attempt to

1. Morgan Stanley Smith Barney LLC, Exchange Act Release No. 78021, Investment Advisers Act Release No. 4415, 2016 WL 3181325 (June 8, 2016).

educate himself about market trends and investment strategies.[2] Though the employee did not have any desire to release the customer information, an outside attacker hacked into his home server and stole the data.[3]

Stories such as the Morgan Stanley breach have captured the public's attention. Hundreds of news articles appear online every week regarding data breaches and cybersecurity in general. Cybercrime has led to millions of dollars in losses for businesses and individuals around the world.[4] In response, state and federal government entities have gotten involved in the fight against data theft and lax security practices.[5]

This Comment will focus on the SEC's role in regulating key investment intermediaries: brokers,[6] dealers,[7] investment companies,[8] and investment advisers.[9] While the SEC has a number of statutes

2. *See* Sentencing Memorandum on Behalf of Defendant Galen Marsh, No. 1:15-cr-00641 (S.D.N.Y. filed Sept. 21, 2015) [hereinafter Sentencing Memorandum], ECF No. 9.

3. *Morgan Stanley*, Exchange Act Release No. 78021, Investment Advisers Act Release No. 4415, 2016 WL 3181325, at *2.

4. *See* PONEMON INST., 2016 COST OF CYBER CRIME & THE RISK OF BUSINESS INNOVATION (2016), http://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf [https://perma.unl.edu/W7M3-S9EL].

5. *See, e.g.*, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015) (upholding the FTC's authority to impose sanctions against a company that suffered a data breach); *Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (Feb. 24, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.unl.edu/AL67-2CPR] (providing a list of all state laws requiring businesses to notify customers about data breaches).

6. "Brokers" are those who, for their business, effect securities transactions for others. *See generally* Securities Exchange Act of 1934 § 3(a)(4), 15 U.S.C. § 78c(a)(4) (2012).

7. "Dealers" are those who engage in the business of buying and selling securities for their own accounts. *See generally* Securities Exchange Act of 1934 § 3(a)(5), 15 U.S.C. § 78c(a)(5) (2012).

8. "Investment company" is a defined term in securities laws; mutual funds are the most commonly recognized type of investment company. *See generally* Investment Company Act of 1940 § 3(a)(1), 15 U.S.C. § 80a-3(a)(1) (2012).

9. "Investment adviser" is a defined term in securities laws; the general idea is that an investment adviser is somebody who gives investment advice as part of a regular business (with certain exceptions). *See generally* Investment Advisers Act of 1940 § 2(a)(11), 15 U.S.C. § 80b-2(a)(11) (2012). For brevity and readability's sake, this Comment will use the blanket term "investment intermediaries" whenever it refers to brokers, dealers, investment companies, and investment advisers all at the same time. Regulation S-P—the primary focus of this Comment—applies to each of these regulated entities, and it will be easier to have one catchall term for most of the discussion. *See* Privacy of Consumer Financial Information (Regulation S-P), 65 Fed. Reg. 40,333 (June 29, 2000) (codified at 17 C.F.R. pt. 248).

and regulations it can use to require data protection,[10] its most obviously applicable regulation is Rule 30 of Regulation S-P, also known as the "Safeguards Rule."[11] The Safeguards Rule requires investment intermediaries to develop policies and procedures "reasonably designed" to protect sensitive client data.[12] Using this rule, the SEC has brought a number of penalty actions against investment intermediaries over the past decade.[13] It has also issued a number of releases, providing additional guidance to regulated entities and informing them of liability they might face in the event of a data breach.[14]

For many reasons, the SEC's approach to data security for investment intermediaries has been laudable. It has recognized the need to protect sensitive client data while still granting investment intermediaries freedom to develop solutions based on their unique situations.[15] The SEC's enforcement approach, however, is inconsistent and, in many cases, overly harsh. Fortunately, the SEC can use its regulatory authority over investment intermediaries to create regulations that promote responsible data security while still being fair to regulated entities.[16]

---

10. *See infra* section IV.B.
11. 17 C.F.R. § 248.30 (2017). The SEC sometimes calls this rule the "Safeguard Rule" (as opposed to the plural Safeguards). This Comment will use the name *Safeguards Rule* because it is the more common term, as well as the term that corresponds more closely with the text of the Act that gave the SEC authority to promulgate the regulation. *See* Gramm–Leach–Bliley Act of 1999, Pub. L. No. 106-102 § 501, 113 Stat. 1338 (codified at 15 U.S.C. § 6801 (2012)). In any case, when the SEC uses a description such as "Rule [number]" in its releases, the number corresponds with the part of the C.F.R. section coming after the period. For example, 17 C.F.R. § 248.10 is Rule 10, 17 C.F.R. § 240.17a-3 is Rule 17a-3, etc.
12. § 248.30(a).
13. *See infra* subsection IV.A.2.; *see also infra* Table 1 (outlining the various actions the SEC has brought under the Safeguards Rule).
14. *See, e.g.*, SEC. & EXCH. COMM'N, IM GUIDANCE UPDATE NO. 2015-02, CYBERSECURITY GUIDANCE (2015) [hereinafter CYBERSECURITY GUIDANCE], https://www.sec.gov/investment/im-guidance-2015-02.pdf [https://perma.unl.edu/JKD7-2EQ2].
15. *See* § 248.30(a); CYBERSECURITY GUIDANCE, *supra* note 14; *see also* NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 2 (2017) ("Organizations will continue to have different risks—different threats, different vulnerabilities, different risk tolerances—and how they implement the practices [described in this framework] will vary."); Vijay Basani, *"Checkbox Compliance" Won't Stop Target-Like Breaches*, USA TODAY (Jan. 20, 2014), https://www.usatoday.com/story/cybertruth/2014/01/20/why-checkbox-compliance-wont-stop-target-like-breaches/4655859 [https://perma.unl.edu/2CLJ-P9TX] (describing how companies should be able to address their own security needs without rigid guidelines because "[t]he 'checkbox' mentality places too much emphasis on Compliance over Risk Management").
16. *See* 15 U.S.C. § 6801(b) (2012) (requiring only that the SEC "establish appropriate standards" regarding protection of customer information).

This Comment begins by giving a background of the threats investment intermediaries face and the regulatory scheme they must navigate. Part II examines some modern threats to sensitive customer data. Part III offers a brief overview of the FTC's role in data-security regulation and a comparison of the FTC's approach to the SEC's. Part IV describes current statutes and SEC regulations that a cyberattack against an investment intermediary might implicate. Part IV also gives an overview of each one of the SEC's enforcement actions under the Safeguards Rule.

Part V rejects the SEC's current approach, focusing primarily on the unfairness of assessing penalties against investment intermediaries that are, in most cases, victims themselves. Part VI offers a three-part solution that will enable the SEC to continue its important work regarding data security while also promoting the market's ability to develop creative solutions to modern threats. Finally, Part VII examines problems that the SEC would create by adopting other proposals for handling data security.

II. MODERN THREATS TO SENSITIVE DATA

Popular legend says that bank robber Willie Sutton, when asked why he chose to rob banks, replied, "That's where the money is."[17] In many ways, modern investment intermediaries present the same type of target to cybercriminals as banks do to robbers. Two things are true about investment intermediaries: (1) they often have large amounts of confidential client data and (2) their clients are people who have money to invest, which makes their information valuable.[18]

While stories about cyberattacks and hackers capture the public's attention, the SEC's regulations in this area of the law are not explicitly about cybersecurity. Rather, they are about customer data security in general.[19] Thus, an investment intermediary that leaves paper files in an unsecure location would be just as liable under the Safeguards Rule as one that fails to take reasonable cybersecurity precautions.[20] However, modern technology has brought about "a previously unimaginable explosion" in the connectivity of devices, including those devices that companies use to store sensitive customer data.[21] With

17. David Martin, *The Ongoing Battle of Cybersecurity*, INSTITUTIONAL INVESTOR (July 12, 2016), http://www.institutionalinvestor.com/blogarticle/3569785/blog/the-ongoing-battle-of-cybersecurity.html#/.WMYqh39Eoil.
18. *See* CYBERSECURITY GUIDANCE, *supra* note 14, at 1; Martin, *supra* note 17.
19. *See, e.g.*, § 248.30.
20. *See, e.g.*, J.P. Turner & Co., LLC, 98 SEC Docket 1729, 2010 WL 2000509 (ALJ May 19, 2010).
21. David X. Martin, *Building a More Effective Cybersecurity Defense*, INSTITUTIONAL INVESTOR (Sept. 8, 2014), http://www.institutionalinvestor.com/blogarticle/3381726/blog/building-a-more-effective-cybersecurity-defense.html#/.WLN4qX9Eoil.

that has come a corresponding explosion of cybercrime—to paraphrase Willy Sutton, cyberspace is "where the [data] is."[22]

Outside actors pose the most obvious source of data-security threats for investment intermediaries. These actors have a number of driving motivations. Some seek to steal sensitive customer data for monetary gain, especially if the information they can take is valuable and easy to use/sell (e.g., credit card information).[23] Others—such as terrorist organizations—might want primarily to cause widespread damage and fear by announcing their attacks on key targets to undermine the public's sense of security.[24] Further, bad actors can use cyberattacks to cause real-world damage, such as a terrorist organization shutting down a power grid.[25] Regardless of the motivation, investment intermediaries are clear targets for cyberattacks because of the valuable information they hold and their importance to the national economy.[26]

Another threat investment intermediaries face—and one that can be easy to overlook—is theft by employees themselves. In fact, employee theft of data led to the biggest settlement for the SEC in any Safeguards Rule proceeding: one million dollars paid by Morgan Stanley.[27] Some employees might steal data for the same reasons as other cybercriminals, such as the desire to sell the information for a profit. Others might steal data for less obvious purposes, such as the employee in the Morgan Stanley breach who took data in an effort to educate himself about market trends.[28]

---

22. *Id.*; *see also* PONEMON INST., *supra* note 4 (showing the rise in losses resulting from cybercrime over the past few years); Lucy L. Thompson, *Insecurity of the Internet of Things*, SCITECH LAW., Spring 2016, at 32 (describing the security risks posed by the amount of connectivity in modern devices).

23. SEC. INDUS. & FIN. MKT. ASS'N (SIFMA), SMALL FIRMS CYBERSECURITY GUIDANCE 4 (2014); *see also Experts Say It's "Highly Likely" North Korea Was Behind the WannaCry Ransomware Attack*, FORTUNE (May 22, 2017), http://fortune.com/2017/05/23/north-korea-wannacry-ransomware-symantec [https://perma.unl.edu/S3Sa-BN66] (describing a worldwide attack involving ransomware—a particular type of attack in which the attacker encrypts the victim's data and only unencrypts it for a fee).

24. *See* Denise Johnson, *Cyber Terrorism Is a Major Concern for U.S. Businesses*, CLAIMS J. (Aug. 15, 2016), http://www.claimsjournal.com/news/national/2016/08/15/272825.htm [https://perma.unl.edu/SND3-VCUV]; Mary Louise Kelly, *ISIS Uses Cyber Capabilities to Attack the U.S. Online*, NPR (Apr. 25, 2016), http://www.npr.org/2016/04/25/475631277/isis-uses-cyber-capabilities-to-attack-the-u-s-online.

25. *See* Kelly, *supra* note 24.

26. *See* CYBERSECURITY GUIDANCE, *supra* note 14.

27. Morgan Stanley Smith Barney LLC, Exchange Act Release No. 78021, Investment Advisers Act Release No. 4415, 2016 WL 3181325, at *5 (June 8, 2016); *see also infra* Table 1 (outlining the various actions the SEC has brought under the Safeguards Rule).

28. *See* Sentencing Memorandum, *supra* note 2.

Another easy-to-overlook threat is the one posed by third-party vendors and service providers. Many companies outsource their back-office processes, such as management of payment systems or other IT services, to third-party vendors.[29] Those vendors often have access to their clients' sensitive data. Thus, those vendors become a weak point—cybercriminals can access a company's data indirectly by breaching the systems of vendors who provide services to the company.[30]

In sum, investment intermediaries must navigate a virtual minefield. Their data is a valuable target for many parties, their employees cannot be fully trusted, and all of their own security efforts can become useless if an outside vendor with access to data suffers a breach. Additionally, the threats these actors pose "are always evolving, increasing in sophistication in order to circumvent the most robust security devices."[31] In many ways, the issue becomes not *whether* an investment intermediary will suffer a breach but rather *when* it will suffer a breach.[32]

III. THE FTC'S APPROACH TO DATA SECURITY

Any discussion of regulatory approaches to data security must first begin with describing the efforts of "the most prominent regulatory agency" to address the issue: the FTC.[33] While few scholarly works address the SEC's approach to data security, several authors recently

29. *See* Sarah Bloom Raskin, Deputy Sec'y, Treasury Dep't, Remarks at the Texas Bankers' Association Executive Leadership Cybersecurity Conference (Dec. 3, 2014), https://www.treasury.gov/press-center/press-releases/Pages/jl9711.aspx [https://perma.unl.edu/YYE6-88GH].

30. OFFICE OF COMPLIANCE INSPECTIONS & EXAMINATIONS, OCIE'S 2015 CYBERSECURITY EXAMINATION INITIATIVE 2 (2015), https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf [https://perma.unl.edu/UE89-9VXH]; Raskin, *supra* note 29; *see also* PONEMON INST., DATA RISK IN THE THIRD-PARTY ECOSYSTEM (2016), http://www.ponemon.org/local/upload/file/Data%20Risk%20in%20the%20Third%20Party%20Ecosystem_BuckleySandler%20LLP%20and%20Treliant%20Risk%20Advisors%20LLC%20Ponemon%20Research%202016%20-%20FINAL2.pdf [https://perma.unl.edu/22JK-ZGS4] (describing the risks posed by companies' relationships with third-party vendors who have access to sensitive records).

31. Brian Contos, *Thinking Outside the Product Box*, CSO ONLINE (Dec. 9, 2015), http://www.csoonline.com/article/3011877/security-awareness/thinking-outside-the-product-box.html [https://perma.unl.edu/U98L-FSYC].

32. As FBI Director James Comey described the situation: "There are two kinds of big companies in the United States. There are those who've been hacked . . . and those who don't know they've been hacked . . . ." Justin (Gus) Hurwitz, *Data Security and the FTC's UnCommon Law*, 101 IOWA L. REV. 955, 957 (2016).

33. Michael Hooker & Jason Pill, *You've Been Hacked, and Now You're Being Sued: The Developing World of Cybersecurity Litigation*, FLA. B.J., July–Aug. 2016, at 30, 38; *see also* Hurwitz, *supra* note 32, at 957 (describing the FTC as being "the primary regulator of online privacy and data security in the United States").

have written about the FTC's enforcement efforts.[34] Those authors' praises and criticisms of the FTC give insights into how the SEC should treat data security issues moving forward.[35]

The FTC's strategy has been primarily to use enforcement actions. Rather than passing regulations regarding data security,[36] it has brought actions against companies with allegedly lax cybersecurity practices in an attempt to build a body of administrative decisions and settlements that other companies can use for guidance.[37] In other words, the FTC is attempting to build "the functional equivalent of common law" in the area of privacy and data security.[38]

The rationale for the FTC's approach lies in the language of its statutory grant of authority and the practical realities of data-security regulation.[39] The FTC's power to regulate data-security practices comes from its consumer-protection mission in section 5 of the FTC Act, which gives it the authority to penalize businesses who engage in "unfair or deceptive acts or practices."[40] In brief, section 5 gives companies two standards with which their conduct must comply: they must not act deceptively or unfairly. Generally, companies engage in "deceptive" acts or practices when they fail to live up to their express promises (e.g., a company falsely claiming that it encrypts customer data).[41] For conduct to be "unfair" it must: (1) cause or be likely to cause substantial injury, (2) not be outweighed by offsetting benefits, and (3) not be reasonably avoidable by consumers.[42]

---

34. *See, e.g.*, Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230 (2015) [hereinafter *Scope and Potential*]; Hurwitz, *supra* note 32.

35. *See infra* Part V.

36. In the Gramm–Leach–Bliley Act, Congress gave the FTC authority to regulate the data security practices of any "financial institution" not subject to the jurisdiction of any other agency. 15 U.S.C. § 6805(a)(7) (2012). The FTC used this authority to promulgate its own version of the Safeguards Rule, found in 16 U.S.C. pt. 314 (2016). However, the primary controversy involving the FTC's data-security enforcement efforts surrounds its use of its section 5 authority, which applies to *all* businesses, rather than merely financial institutions. *See generally* Hurwitz, *supra* note 32, at 1003–05 (discussing FTC jurisdictional concerns).

37. *See* Hurwitz, *supra* note 32, at 966–67. *See generally* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014) [hereinafter *Common Law of Privacy*].

38. *Common Law of Privacy*, *supra* note 37, at 619.

39. *See generally* Hurwitz, *supra* note 32, at 1008; *Common Law of Privacy*, *supra* note 37, at 656.

40. 15 U.S.C. § 45(a) (2012 & Supp. 2014); Hurwitz, *supra* note 32, at 964.

41. Hurwitz, *supra* note 32, at 965, 968 n.58; *Common Law of Privacy*, *supra* note 37, at 599; *see, e.g.*, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015); GeoCities, 127 F.T.C. 94 (1999).

42. § 45(n); Hurwitz, *supra* note 32, at 965.

Section 5's statutory grant of authority for the FTC to protect consumer interests is vague, especially under the unfairness prong.[43] What types of data breaches would constitute substantial injuries? What makes a data-security practice likely to cause such an injury? What types of offsetting benefits might weigh against additional efforts toward data security? What steps might reasonable consumers take to avoid substantial injuries resulting from data breaches? In short, section 5 does not resemble anything close to a bright-line rule. Thus, the FTC's jurisprudence on data-security matters has been analogous to the development of rules under the common law: it "began very generally" with relatively easy cases involving deception before moving into cases that were more complex.[44]

In some ways, the constant, rapid evolution of technology and cyber threats make a case-by-case approach to regulation necessary.[45] Proponents of the FTC's efforts describe its approach as one that provides "flexibility to adapt to new situations" in a way that static regulations do not.[46] Further, they argue that FTC enforcement actions, when viewed collectively, give companies "a rather detailed list of inadequate security practices."[47] Therefore, businesses *should* be on notice of the general types of practices that could lead to penalty actions. However, some unpredictability remains: businesses can never be completely certain whether the FTC will find their data-security efforts unfair.[48] In fact, a company cannot even be certain the FTC will

43. *Common Law of Privacy*, *supra* note 37, at 649. The deception prong of section 5 tends to be the more straightforward—and thus less controversial—of the two. Hurwitz, *supra* note 32, at 1015. Either a company lied about its data-security practices or it did not. Granted, certain fact-based questions remain: deceptions must be material (similar standard to securities laws) and they must be likely under the circumstances in which they are made to mislead reasonable consumers. FTC v. Stefanchik, 559 F.3d 924, 928 (9th Cir. 2009). However, the relative clarity of deception as opposed to unfairness, combined with the ability to bring unfairness claims against any company regardless of its statements to consumers, means that most of the FTC's "data security jurisprudence has been developed under . . . [its] 'unfairness' authority." Hurwitz, *supra* note 32, at 964.

44. *Common Law of Privacy*, *supra* note 37, at 649–50; *see also* Hurwitz, *supra* note 32, at 969 ("[The FTC's] initial cases focused on deception, where companies failed to live up to their stated security policies.").

45. *See Scope and Potential*, *supra* note 34, at 2245, 2264–65; *cf.* Hurwitz, *supra* note 32, at 1008 ("[T]he basic rationale for allowing agencies to develop rules through adjudication is that, in some instances, it is difficult to craft ex ante rules.").

46. *Scope and Potential*, *supra* note 34, at 2265. *See generally* Kenneth A. Bamberger & Deirdre K. Mulligan, *New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States: An Initial Inquiry*, 33 LAW & POL'Y 477 (2011) (describing the policies underlying the FTC's efforts in consumer privacy and data security).

47. *Common Law of Privacy*, *supra* note 37, at 650–55 (providing a list of security practices the authors pulled from various FTC decisions).

48. Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 273–75 (2010).

follow its previous decisions, given that they have no binding precedential value.[49] Still, some proponents argue that this built-in unpredictability is a good thing because if a business cannot find bright-line standards with which to comply, it will attempt instead to adopt the strongest possible data-security standards in order to avoid FTC enforcement.[50]

Critics of the FTC's data-security enforcement, however, point out numerous flaws in its approach. First, Congress has never explicitly ordered the FTC to use its section 5 to regulate data-security practices—a key omission if the FTC wants the public to regard its actions as legitimate.[51] Rather, the FTC took its general authority to regulate unfair acts and practices and stretched it into a new area. The result is that "most consumers and businesses do not naturally think of [the FTC] as a data security regulator—let alone as the nation's primary source of data security protections."[52] If businesses do not regard the FTC as a data-security regulator, they will not be likely to seek its guidance on such matters.[53]

Second, the FTC's enforcement strategy raises fairness concerns. To begin with, the FTC's authority under section 5 can extend to every single business in the United States.[54] Unfortunately, while almost all businesses maintain electronic records, very few are able to afford the type of legal counsel necessary to navigate the FTC's quasi-common law.[55] To compound the problem, relatively few attorneys have expertise in FTC data-security practices or understand the problem in the first place—most businesses will focus on complying with state

49. Hurwitz, *supra* note 32, at 987.

50. Amicus Curiae Brief of Eight Privacy and Security Law Professors in Support of Respondent at 9–12, LabMD, Inc. v. FTC, No. 16-16270 (11th Cir. Sept. 29, 2016), 2017 WL 664269 [hereinafter Security Law Professors Brief].

51. *See* Hurwitz, *supra* note 32, at 1005.

52. *Id.* at 1011. Some reason exists to believe this might change, especially if the FTC continues bringing high-profile cases. In the aftermath of the Third Circuit's *Wyndham* decision, numerous articles discussed the FTC's power to bring actions against companies for alleged failures in data protection. *See, e.g.*, Grant Gloss, *FTC Can Bring Down the Hammer on Companies with Sloppy Cybersecurity, Court Rules*, COMPUTERWORLD (Aug. 24, 2015), http://www.computerworld.com/article/2975054/security/ftc-can-bring-down-the-hammer-on-companies-with-sloppy-cybersecurity-court-rules.html [https://perma.unl.edu/X2D8-7ESA]; Andy Greenberg, *Court Says the FTC Can Slap Companies for Getting Hacked*, WIRED (Aug. 24, 2015), https://www.wired.com/2015/08/court-says-ftc-can-slap-companies-getting-hacked [https://perma.unl.edu/VN9Z-2XJJ]. Nevertheless, an explicit grant of authority from Congress to police all businesses' data-security practices would confer legitimacy on the FTC's efforts in a way that its current approach lacks. *Cf. infra* subsection IV.A.1. (describing the SEC's statutory mandate under the Gramm–Leach–Bliley Act).

53. Hurwitz, *supra* note 32, at 1012.

54. *See id.* at 1003–05.

55. *Id.* at 1003.

laws or industry-specific regulators.[56] Further, companies that violate the FTC's uncertain standards face considerable penalties. Although the FTC's ability to assess monetary fines is limited, the standard settlement between the FTC and businesses is a twenty-year consent order, during which time the business must agree to "ongoing monitoring and security audits and the threat of substantial fines for future breaches."[57]

Third, the FTC's methods raise doubts about the quality of any rules it develops. Although the FTC has explicitly referred to its efforts "as developing a 'common law' body of rules,"[58] critics have pointed out numerous differences that call the analogy into question. Chief among these differences is that "[t]he FTC is not an independent adjudicator; it is a party to the enforcement actions it brings."[59] Thus, the FTC has conflicting interests. The common law works as a system to develop rules over time because judges are impartial and must hear any case brought before them.[60] Litigants have financial incentives to settle easy cases but devote time and resources into fighting harder cases in order to determine what legal principles the court will adopt.[61] When the FTC brings its data-security actions, it is able to choose which cases it wants to hear—a power it uses to further its own interests as an enforcer of data security-standards.[62] Further, businesses have strong financial and reputational incentives to quickly settle with the FTC regardless of the merits of their cases. A business that wishes to challenge an FTC proceeding must spend money on legal fees, and it also must expect that news about its situation—including news of any embarrassing data breaches—will appear in various media outlets.[63] Therefore, the FTC does not often hear alternative points of view before issuing its orders.[64] In short, critics describe how the FTC brings actions in which it assumes the conclusion—the business *must* have had insufficient data security—and uses its enforce-

56. *Id.*

57. *Id.* at 958, 1003. Even proponents of the FTC's approach to data security concede these twenty-year consent orders can be "overkill" in many—if not most—cases. *See Scope and Potential*, *supra* note 34, at 2297.

58. Hurwitz, *supra* note 32, at 966.

59. *Id.* at 984. One other issue is that stare decisis does not bind agencies in the same way as it does courts, meaning agencies generally can change their views at any time. *Id.* at 987.

60. *Id.* at 983–84.

61. *Id.* at 982–83.

62. *Id.* at 984.

63. *See, e.g.*, Gloss, *supra* note 52 (describing the FTC's victory over Wyndham Worldwide Corp.).

64. Hurwitz, *supra* note 32, at 985–86 (describing the FTC's "unprecedented success rate in its adjudications" and the incentives businesses have to settle).

ment powers to develop the law in a direction it has unilaterally deemed appropriate, ignoring other considerations and perspectives.[65]

IV. THE SEC'S APPROACH TO DATA SECURITY

In contrast to the FTC's "regulate everybody" approach, the SEC has kept its efforts comparatively focused. Section 501 of the Gramm–Leach–Bliley Act (GLBA) gave the SEC an explicit mandate to regulate data-security standards for investment intermediaries.[66] The SEC used this grant of authority to promulgate the Safeguards Rule, its main tool for developing and enforcing data-security standards.[67] Beyond its regulations and enforcement actions, the SEC has attempted to assist investment intermediaries in creating quality data-security practices through nonpunitive measures, such as guidance updates and voluntary surveys.[68] The SEC's data-security efforts fall into two broad categories: (1) its guidance and enforcement efforts regarding the Safeguards Rule and (2) its guidance regarding other statutes and regulations.

A. The Safeguards Rule

The Safeguards Rule is the SEC's clearest and most powerful data-protection regulation. It imposes a requirement on investment intermediaries to "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information."[69] Investment intermediaries must "reasonably" design these policies and procedures to protect customer data; merely quoting the text of the Safeguards Rule verbatim in an employee manual is insufficient.[70]

This section explains the SEC's Safeguards Rule development in two broad parts. First, it describes the SEC's adoption of the Safe-

65. *Id.* at 986–87; *see also id.* at 980 (describing how the common law can lead to development of good principles over time, but only where it results in a stable set of principles without a predetermined outcome).

66. Gramm–Leach–Bliley Act of 1999, Pub. L. No. 106-102 § 501, 113 Stat. 1338 (codified at 15 U.S.C. § 6801 (2012)).

67. Privacy of Consumer Financial Information (Regulation S-P), 65 Fed. Reg. 40,333 (June 29, 2000) (codified at 17 C.F.R. pt. 248).

68. *See, e.g.*, OFFICE OF COMPLIANCE INSPECTIONS & EXAMINATIONS, CYBERSECURITY EXAMINATION SWEEP SUMMARY (2015) [hereinafter OCIE SWEEP SUMMARY], https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf [https://perma.unl.edu/J2PD-UY4Q]; OFFICE OF COMPLIANCE INSPECTIONS & EXAMINATIONS, OBSERVATIONS FROM CYBERSECURITY EXAMINATIONS (2017) [hereinafter OCIE 2017 UPDATE], https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf [https://perma.unl.edu/7EHZ-27V8]; CYBERSECURITY GUIDANCE, *supra* note 14.

69. 17 C.F.R. § 248.30(a) (2017).

70. *Id.*; *see* J.P. Turner & Co., LLC, 98 SEC Docket 1729, 2010 WL 2000509, at *6–7 (ALJ May 19, 2010).

guards Rule through its rulemaking procedures. Second, it examines the eleven actions the SEC has brought using the Safeguards Rule. Although the SEC has attempted to publicize some of its actions under the Safeguards Rule,[71] nobody has yet put together a comprehensive overview of all the SEC's actions. However, understanding the SEC's approach and some of the problems with it must begin with a review of how the SEC has actually developed and used the Safeguards Rule over time.

1. Development of the Safeguards Rule

The SEC promulgated Regulation S-P, including the Safeguards Rule, in response to Congress's statutory mandate in the GLBA.[72] Regulation S-P focuses on three broad topics. First, it requires investment intermediaries to adopt policies and procedures to protect customer data (i.e., the Safeguards Rule).[73] Second, it generally requires investment intermediaries to disclose their data-privacy policies and practices to customers—both at the start of the customer relationship and annually thereafter.[74] Third, it establishes limits on when investment intermediaries can disclose their customers' nonpublic personal information to nonaffiliated third parties.[75]

Surprisingly, the original Regulation S-P proposing release had very little to say regarding the Safeguards Rule.[76] The SEC merely explained that it was not prescribing specific policies or procedures to adopt. Rather, the SEC "believe[d] it more appropriate for each institution to tailor its policies and procedures to its own systems of information gathering and transfer and the needs of its customers."[77] The adopting release also had very little to say about the Safeguards Rule, only pointing out that commenters supported the regulation as proposed.[78] The only concern some commentators raised was whether related investment intermediaries in a fund complex could satisfy the

71. *See, e.g.*, Press Release, Sec. & Exch. Comm'n, SEC Charges Investment Adviser with Failing to Adopt Proper Cybersecurity Policies and Procedures Prior to Breach (Sept. 22, 2015) [hereinafter R.T. Jones Release], https://www.sec.gov/news/pressrelease/2015-202.html [https://perma.unl.edu/BE58-37TD].

72. Privacy of Consumer Financial Information (Regulation S-P), 65 Fed. Reg. at 40,334.

73. § 248.30(a).

74. 17 C.F.R. §§ 248.4–.5 (2017).

75. 17 C.F.R. § 248.10 (2017) (imposing requirements with which investment intermediaries must comply before they can transfer customer information); 17 C.F.R. § 248.7 (2017) (defining the form of the opt-out notice that investment intermediaries must provide customers before transferring personal data).

76. *See* Privacy of Consumer Financial Information (Regulation S-P), 65 Fed. Reg. 12,354, 12,365 (Mar. 8, 2000).

77. *Id.*

78. *See* Privacy of Consumer Financial Information (Regulation S-P), 65 Fed. Reg. 40,333, 40,357 (June 29, 2000) (codified at 17 C.F.R. pt. 248).

rule by adopting a single set of policies and procedures.[79] The SEC's response was that it believed intermediaries in a fund complex could satisfy the regulation as proposed, provided their combined policies were "appropriate for each institution to which they apply."[80]

The original version of the Safeguards Rule differed from its current form in one key respect: it did not require investment intermediaries to put their policies and procedures in writing.[81] This changed in 2004 when the SEC made its first—and only—amendment to the Safeguards Rule. Section 216 of the Fair and Accurate Credit Transactions Act of 2004 required the SEC (among other agencies) to pass regulations regarding proper disposal of certain consumer reports.[82] While the SEC was promulgating its new disposal rule,[83] it also updated the original Safeguards Rule to require companies to adopt written procedures.[84] While one purpose for the change was to encourage compliance (given the difficulty in protecting customer data in a meaningful way without written policies and procedures), the primary motivation was to make the SEC's oversight role easier.[85] Checking to see whether written policies and procedures exist is easier to do than interviewing individual employees of an investment intermediary to see whether they follow any unwritten practices regarding data security.[86]

A few aspects of the SEC's Safeguards Rule are worth noting. First, the SEC has been mindful of the costs that investment intermediaries will incur, keeping their needs in mind while developing the Safeguards Rule.[87] Second, the public was generally supportive of the SEC's proposed rule and amendments—the only real question that arose during the rulemaking process was whether various institutions in a fund complex could have a uniform policy.[88] Third, the SEC's approach has been very hands off, leaving investment intermediaries great freedom to design their policies around their own specific needs. In fact, the SEC expressly refused to amend its Safeguards Rule to make it closer to the FTC's version of the rule, which

79. *See id.*

80. *Id.*

81. *Id.* at 40,371.

82. Disposal of Consumer Report Information, 69 Fed. Reg. 71,321 (Dec. 8, 2004) (codified at 17 C.F.R. § 248.30).

83. 17 C.F.R. § 248.30(b) (2017).

84. Disposal of Consumer Report Information, 69 Fed. Reg. at 71,325.

85. *Id.*

86. *Cf. infra* subsection VI.A.4. (prescribing a recordkeeping requirement as an amendment to the Safeguards Rule).

87. *See, e.g.*, Disposal of Consumer Report Information, 69 Fed. Reg. at 71,326.

88. *See* Privacy of Consumer Financial Information (Regulation S-P), 65 Fed. Reg. 40,333, 40,357 (June 29, 2000) (codified at 17 C.F.R. pt. 248).

specified elements that regulated financial institutions must include in their plans.[89]

2. Safeguards Rule Enforcement Actions

Although the SEC adopted the Safeguards Rule in 2000—later clarifying it in 2004 to require written policies—it did not bring any enforcement actions under it for almost eight years. Since then, it has brought a total of eleven enforcement actions against various investment intermediaries and their employees.[90] Only two of the decisions have gone before an administrative law judge (ALJ); the rest quickly settled.[91] However, a few things stand out about these actions. First, violations of the Safeguards Rule seem to be secondary considerations in several of the decisions, with the primary violations being for willing but unauthorized transfers of information to unaffiliated third parties.[92] Second, the decisions often do not explain why certain practices were unsafe, even where the only alleged violation was of the Safeguards Rule and the penalty was substantial.[93]

a. NEXT Financial Group

In 2008, the SEC brought its first enforcement action involving the Safeguards Rule.[94] The defendant, NEXT Financial Group, was a broker-dealer that had an aggressive system in place for recruiting registered representatives.[95] One of its requirements was that new representatives provide it with information about all of their personal

89. 16 C.F.R. § 314.4 (2017); Disposal of Consumer Report Information, 69 Fed. Reg. at 71,325. The SEC did propose a regulation that would have set express standards for the Safeguards Rule. Part 248—Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information, 73 Fed. Reg. 13,691 (May 12, 2008). However, the SEC withdrew the proposed regulation in 2013. Since then, the SEC has not proposed any additional amendments to the Safeguards Rule.

90. The Appendix of this Comment contains a table showing key details from each of the SEC's eleven enforcement actions. *See infra* Table 1.

91. J.P. Turner & Co., 98 SEC Docket 1729, 2010 WL 2000509 (ALJ May 19, 2010); NEXT Fin. Grp., 93 SEC Docket 1369, 2008 WL 2444775 (ALJ June 18, 2008); *see* Hurwitz, *supra* note 32, at 985–86 (describing the reasons companies quickly settle in these types of agency actions).

92. *See* 17 C.F.R. § 248.10 (2017). Rule 10 applies when an investment intermediary *discloses* a customer's private information to a third party. Thus, the text of the rule does not seem to apply to involuntary data breaches, nor has the SEC used it in any case other than those in which the investment intermediary voluntarily gave information to a third party without customer authorization.

93. *See, e.g.*, Morgan Stanley Smith Barney LLC, Exchange Act Release No. 78021, Investment Advisers Act Release No. 4415, 2016 WL 3181325 (June 8, 2016) (reaching a one-million-dollar settlement for an alleged violation of the Safeguards Rule).

94. *NEXT Fin.*, 93 SEC Docket 1369, 2008 WL 2444775.

95. *See id.* at *9–10.

customers from their previous firms.[96] NEXT did not determine whether those customers consented to have the representatives transfer the information to NEXT.[97] Further, NEXT occasionally required recruits to log into their current brokerage firms' sites so it could collect customer data.[98] Once it had the data, NEXT would store it indefinitely on the firm's common server—a server accessible from outside the office by employees with proper clearance.[99] In addition to its practices for incoming representatives, NEXT allowed any departing representatives to take their personal customer files without first obtaining customer approval.[100]

The SEC brought a claim against NEXT for multiple violations of Regulation S-P. The main violation was the unauthorized transfers of data without customer permission—both NEXT's own transfers and its requirement that incoming representatives bring data about their old accounts.[101] The ALJ agreed with the SEC that NEXT's actions were a straightforward violation of Rule 10 of Regulation S-P (regarding unauthorized data transfers between unaffiliated parties).[102]

In addition to the Rule 10 violation, the SEC tacked on a Safeguards Rule violation, claiming that NEXT's practices involving data transfers left customer data vulnerable to unauthorized access.[103] The ALJ described the procedure for Safeguards Rule actions, saying that the initial burden is on the defendant to show it adopted policies and procedures regarding safeguarding customer information and kept them up-to-date.[104] If the defendant makes that showing, the burden is on the SEC to establish "through competent evidence" that the policies were not reasonable.[105] In NEXT's case, the ALJ decided that NEXT had not maintained appropriate policies—although it had privacy policies, NEXT did not amend them after adoption of Regulation S-P to include information about customer data transfers.[106] Thus, the ALJ did not answer the question of whether NEXT's practices actually put customer data at risk.[107] Mostly for its violations of Rule

96. *Id.* at *10.
97. *Id.* at *11.
98. *Id.* at *11–12.
99. *Id.* at *12.
100. *Id.*
101. *See id.* at *32, *36–37. NEXT's primary liability was for its own transfers of data. Its secondary liability was for the incoming representatives' transfers of data—aiding and abetting other broker-dealers' violations of Rule 10.
102. *Id.* at *32–33.
103. *Id.* at *33–34.
104. *See id.*
105. *Id.* at 33.
106. *Id.* at *13–14, 34.
107. The ALJ accepted the SEC's argument that NEXT acted negligently in adopting its early policies. *Id.* at *35. But the ALJ rejected the SEC's claim that the Safeguards Rule required NEXT to encrypt its e-mail traffic, finding the SEC had not

10, but also partially for its violation of the Safeguards Rule, NEXT had to pay a fine of $125,000.[108]

b. LPL Financial Corp.

A few months later, the SEC brought its second action involving the Safeguards Rule.[109] This action—against LPL Financial Corp.—stands out for three reasons. First, it actually involved a data breach: an outside attacker got access to LPL's records and even attempted to place unauthorized trades for customers. Second, LPL's only alleged violation was of the Safeguards Rule. Third, this was the SEC's second-biggest settlement under the Safeguards Rule ($275,000).[110]

LPL had Safeguards Rule policies and procedures in place. However, the SEC determined these policies were insufficient to protect customer data. In particular, LPL had an online portal that its representatives used to handle customer accounts and transactions. This online portal had several security deficiencies: (1) it did not establish minimum-strength requirements for passwords, (2) passwords would not automatically expire after a set time, (3) users could not set their own passwords, (4) it would not lock users out after numerous failed login attempts, and (5) users had to manually log out because the portal would only automatically log them off after eight hours of inactivity.[111] Further, more than three hundred LPL employees had access to a master user–password list for the online portal, including employees who likely did not need that information.[112]

LPL's auditors discovered these security problems in mid-2006.[113] They sent their findings to management, who began taking steps to fix the issues (doing cost–benefit analyses of LPL's options) in early- to mid-2007.[114] Unfortunately, before LPL fully addressed the issues, an outside attacker accessed the online portal. The attacker obtained access to at least ten thousand customers' information and attempted to place over $700,000 in unauthorized trades.[115] LPL managed to block most of the trades and even reimbursed customers for all lost funds (nearly $100,000 worth).[116] Importantly, the SEC's main concerns with LPL seemed not to be a lack of action but rather a lack of *quick*

given adequate advice on the matter that would have put NEXT on notice. *Id.* at *35–36.

108. *Id.* at *49–50
109. LPL Fin. Corp., Exchange Act Release No. 58515, Investment Advisers Act Release No. 2775, 2008 WL 4179915 (Sept. 11, 2008).
110. *See id.* at *6.
111. *Id.* at *3.
112. *Id.*
113. *Id.* at *4.
114. *Id.*
115. *Id.* at *2.
116. *Id.*

action.[117] In attempting to fix its security problems, LPL moved too slowly to prevent the SEC from imposing a massive $275,000 penalty as part of the settlement agreement.

c. J.P. Turner & Co. *and* Stephen Bauman

The SEC's third and fourth actions were against J.P. Turner & Co. and its acting chief compliance officer.[118] The action against Stephen Bauman was relatively straightforward: her job was to ensure J.P. Turner was complying with all securities laws and regulations, making her liable for aiding and abetting J.P. Turner's failures.[119] She settled quickly. The only interesting thing about Bauman's case is that the SEC did not fine or censure her. Her only sanction was that she had to desist from further violations of the Safeguards Rule.[120]

J.P. Turner, on the other hand, did not settle with the SEC. In fact, it was the only case other than *NEXT Financial* to go before an ALJ. The SEC first became aware of J.P. Turner's Safeguards Rule failings in late 2006. A J.P. Turner employee left several thousand sensitive customer records, including social security numbers and bank account information, in boxes on the street curb outside of his suburban Atlanta home.[121] A branch officer for the SEC's Office of Compliance Inspections and Examinations saw a report about the incident on the local news, and the SEC began its investigation.[122]

The SEC discovered that J.P. Turner's supervisory manuals did not have any references to safeguarding customer data.[123] When, in 2006, J.P. Turner finally adopted written policies in its manuals, those policies consisted only of an almost-verbatim quote of the Safeguards Rule.[124] The policies specified that Bauman would be in charge of developing specific rules, but as far as the SEC could determine, Bauman had not done so.[125] J.P. Turner made a few policy statements about data security available to customers, but those documents never specified how J.P. Turner would protect customer data—only that it purportedly understood the general importance of protecting data.[126]

117. *See id.* at *4 ("Nonetheless, LPL failed to take *immediate* corrective action." (emphasis added)).
118. J.P. Turner & Co., LLC, 2009 WL 2138674 (July 17, 2009); Stephen Cheryl Bauman, Exchange Act Release No. 60326, 2009 WL 2138437 (July 17, 2009).
119. *See Bauman*, Exchange Act Release No. 60326, 2009 WL 2138437.
120. *Id.* at *3.
121. J.P. Turner & Co., LLC, 98 SEC Docket 1729, 2010 WL 2000509, at *4 (ALJ May 19, 2010).
122. *Id.*
123. *Id.* at *5–6.
124. *Id.* at *6.
125. *Id.*
126. *Id.* at *14–15.

In short, J.P. Turner did not fail to adopt *reasonable* policies; it failed to adopt *any* policies. Notwithstanding this failure—and despite the firm's knowledge of the Safeguards Rule and Regulation S-P in general—the ALJ refused to find that J.P. Turner's employees acted recklessly or deliberately in ignoring the written-policies-and-procedures requirement.[127] In particular, the ALJ pointed to the general policy statements J.P. Turner had made available to customers, saying these evidenced "attempts to comply with Regulation S-P and specifically, though less effectively, with the Safeguard[s] Rule."[128] Thus, the ALJ declared that J.P. Turner had only committed a first-tier violation under the Exchange Act and imposed the maximum statutory penalty of $65,000.[129]

d. Commonwealth Equity Services

Between its initial order in the *J.P. Turner* case and the ALJ's ultimate decision, the SEC brought its fifth Safeguards Rule action. The defendant, Commonwealth Equity Services (CES), suffered a cyber attack in November 2008.[130] The attacker got access to information from 368 accounts, including partial social security numbers (only the last four digits), account types, cash balances, and owner net worth.[131] The intruder attempted to place stock orders in eight of the accounts, totaling more than $523,000 in unauthorized purchases.[132] However, CES caught the breach within minutes, ultimately cancelling the unauthorized trades and absorbing $8,000 in losses.[133] CES quickly notified the account owners, law enforcement groups, and the SEC.[134]

Like LPL Financial, CES had written policies and procedures in place when it suffered a breach. However, the SEC found two problems with the policies. First, CES did not mandate that employees have antivirus software.[135] This fact was important because the breached computer did not have any kind of antivirus program installed. Second, CES did not have policies requiring its IT department to follow up with potential issues.[136] The employee who suffered the breach contacted the IT department several times in the months lead-

127. *Id.* at *17–18.
128. *Id.* at *18.
129. *Id.*; *see also* Securities Exchange Act of 1934 § 21B, 15 U.S.C. § 78u-2 (2012) (establishing the maximum penalties the SEC can assess for different violations—17 C.F.R. § 201.1001 (2017) adjusts these amounts to account for inflation).
130. Commonwealth Equity Servs., LLP, Exchange Act Release No. 60733, Investment Advisers Act Release No. 2929, 2009 WL 3100577, at *2 (Sept. 29, 2009).
131. *Id.* at *2–3.
132. *Id.* at *3.
133. *Id.*
134. *Id.*
135. *Id.*
136. *Id.*

ing up to the breach, complaining that his computer had a virus.[137] But despite these calls, the IT department's only recommendations were that the employee (1) install antivirus software and (2) take his computer to a local shop.[138] LPL agreed to settle with the SEC, paying a penalty of $100,000.[139]

e. GunnAllen Financial

Marc Ellis, Frederick Kraus, and David Levine were all employees of GunnAllen Financial, Inc., a former broker-dealer.[140] GunnAllen, before ceasing operations, allegedly breached the Safeguards Rule and Rule 10 (involving unauthorized data transfers) in four ways. First, GunnAllen's only policy regarding safeguarding information was insufficient, merely reciting the Safeguards Rule text and providing examples of procedures the firm *might* adopt.[141] Second, somebody stole several of GunnAllen's laptops, but nobody attempted to locate the laptops or amend the firm's safeguard policies in response to the thefts.[142] Third, as part of GunnAllen's winding up, Kraus authorized Levine to download sixteen thousand customer files to a flash drive that Levine then took to his new employer.[143] Fourth, GunnAllen's employees never updated its policies to cover protection of data during its winding-up phase.[144]

Ellis was liable for the firm's failures to adopt meaningful policies or keep them updated before its winding up.[145] He had been GunnAllen's chief compliance officer, in charge of making sure the firm was accomplishing its obligations under securities laws. The SEC indicated that he should have directed the firm to amend its policies in response to the laptop thefts.[146] Thus, he was liable for aiding and abetting GunnAllen's Safeguards Rule violations. Unlike the other two, Ellis did not face liability for violations of any other rules (such as Rule 10), and he ultimately settled for $15,000.[147]

137. *Id.*
138. *Id.*
139. *Id.* at *4.
140. Marc A. Ellis, Exchange Act Release No. 64220, 2011 WL 1325566 (Apr. 7, 2011); Frederick O. Kraus, Exchange Act Release No. 64221, 2011 WL 1325567 (Apr. 7, 2011); David C. Levine, Exchange Act Release No. 64222, 2011 WL 1325568 (Apr. 7, 2011). Because GunnAllen had wound up operations, the SEC chose only to bring penalty actions against the three employees.
141. *Ellis*, Exchange Act Release No. 64220, 2011 WL 1325566, at *2.
142. *Id.* at *3. Additionally, GunnAllen's employees never attempted to contact the customers whose data was on the laptops. *Id.*
143. *Kraus*, Exchange Act Release No. 64221, 2011 WL 1325567, at *1; *Levine*, Exchange Act Release No. 64222, 2011 WL 1325568, at *1.
144. *Levine*, Exchange Act Release No. 64222, 2011 WL 1325568, at *5.
145. *Ellis*, Exchange Act Release No. 64220, 2011 WL 1325566, at *4.
146. *Id.*
147. *Id.*

Kraus, on the other hand, faced liability for violations of both the Safeguards Rule and Rule 10.[148] His Rule 10 liability resulted from his granting Levine permission to take customer records to a new employer. The SEC's discussion of how Kraus violated the Safeguards Rule was limited, only saying that he "knowingly placed customer information at substantial risk of unauthorized access and misuse" by allowing employees to take data.[149] By allowing the transfers, according to the SEC, he aided and abetted GunnAllen's Safeguards Rule violations.[150] Kraus settled with the SEC for $20,000.[151]

Finally, Levine faced liability for violations of both the Safeguards Rule and Rule 10. The Rule 10 violation was obvious enough: Levine was the sales manager who downloaded the customer files to take to his new employer. Additionally, the SEC's theory for how Levine violated the Safeguards Rule was essentially the same as it had been for Kraus.[152] Levine's sales manager position made him, according to the SEC, a "senior officer" of GunnAllen.[153] As a senior officer, he was liable as an aider and abettor of GunnAllen's alleged failures.[154] Levine settled with the SEC for $20,000.[155]

f. R.T. Jones Capital Equities Management

After its three actions in the *GunnAllen* case, the SEC did not bring any further actions under the Safeguards Rule until 2015. At that time, it brought a well-publicized case against R.T. Jones Capital Equities Management, a registered investment adviser.[156] *R.T. Jones* was another case that developed in the aftermath of a data breach. R.T. Jones had approximately eight thousand clients for whom it provided advice regarding retirement plans.[157] In turn, each of these clients provided R.T. Jones with information about their individual plan participants (more than 100,000 individuals).[158] R.T. Jones stored this information on its private servers.[159]

In mid-2013, R.T. Jones discovered that an outside attacker had accessed its private server, potentially compromising all the data.[160]

148. *Kraus*, Exchange Act Release No. 64221, 2011 WL 1325567, at *4–5.
149. *Id.* at *5.
150. *Id.*
151. *Id.*
152. *See* David C. Levine, Exchange Act Release No. 64222, 2011 WL 1325568, at *5 (Apr. 7, 2011).
153. *Id.*
154. *Id.*
155. *Id.*
156. *See* R.T. Jones Release, *supra* note 71.
157. R.T. Jones Capital Equities Mgmt., Inc., Investment Advisers Act Release No. 4204, 2015 WL 5560846, at *2 (Sept. 22, 2015).
158. *Id.*
159. *Id.*
160. *Id.*

In response, R.T. Jones quickly hired several cybersecurity firms to assess the damage. It also notified all of the potentially affected individuals.[161] Despite their efforts, the cybersecurity firms could not accurately assess the scope of the damage—the hackers had destroyed the server's log files, leaving no indications of how long they had access to the data or what data they might have taken.[162] The cybersecurity firms were able to discover, however, that all the attacks had originated from IP addresses in mainland China.[163]

In response to the incident, the SEC launched an investigation of R.T. Jones, ultimately discovering that R.T. Jones failed to have any written policies in place for safeguarding customer data.[164] The SEC offered suggestions as to what R.T. Jones's policies might have included: "conducting periodic risk assessments, employing a firewall to protect the web server containing client [information], encrypting client [information] stored on that server, or establishing procedures for responding to a cybersecurity incident."[165] Somewhat inconsistently, the final sentence of the order suggests that R.T. Jones actually did have policies in place: "Taken as a whole, R.T. Jones's policies and procedures for protecting customer records and information were not reasonable to safeguard customer information."[166] But given that most of the order talks about R.T. Jones not having policies, and it never discusses specific policies R.T. Jones actually had, presumably R.T. Jones's failure was that it had no policies.[167] Regardless, R.T. Jones settled with the SEC for $75,000.[168]

g. Craig Scott Capital

The SEC's next action came in 2016. Like several of its other decisions,[169] the primary violation in this case was not of the Safeguards Rule. Rather, Craig Scott Capital, LLC's (CSC) primary violation was that it was not keeping certain records as required by the Exchange

161. *Id.*

162. *Id.*

163. *Id.*

164. *Id.* at *3.

165. *Id.*

166. *Id.*

167. *See* Alessandra Malito, *SEC Nails Advisory Firm for Cybersecurity Failure Before Data Breach*, INVESTMENTNEWS (Sept. 22, 2015), http://www.investmentnews.com/article/20150922/FREE/150929966/sec-nails-advisory-firm-for-cybersecurity-failure-before-data-breach [https://perma.unl.edu/HJ56-BLDN] ("The firm never adopted written policies and procedures . . . .").

168. *R.T. Jones*, Investment Advisers Act Release No. 4204, 2015 WL 5560846, at *4.

169. *See, e.g.*, NEXT Fin. Grp., Inc., 93 SEC Docket 1369, 2008 WL 2444775 (ALJ June 18, 2008).

Act.[170] CSC's employees set up an eFax system that would automatically convert all regular faxes into electronic files.[171] The system would then route those files to various e-mail addresses. However, a few of the e-mail addresses CSC used were not firm addresses; they were personal addresses of two employees.[172]

Over a four-year period, thousands of e-mails went through this eFax system.[173] While these faxes routinely contained private customer data, CSC did not have a system in place for storing and maintaining records of these communications when they went to the nonfirm e-mails.[174] Further, while CSC did have written policies as required by the Safeguards Rule, none of the policies dealt with the eFax system.[175] Other deficiencies with the policies were that (1) they did not designate an officer who would be in charge of compliance, (2) they contained blank spaces (e.g., "[The Firm] has adopted procedures to protect customer information, including the following: [methods]"), and (3) they did not require employees to encrypt data.[176] CSC ultimately settled with the SEC for $100,000.[177]

In addition to the firm itself, the SEC brought claims as part of the same action against CSC's two cofounders, who were also serving as CSC's chief compliance officer and chief operating officer at the time.[178] Despite the cofounders' positions of power within CSC, the SEC only found them liable for CSC's failure to comply with the record-maintenance rules—neither was liable for the alleged Safeguards Rule violations.[179] In its order, the SEC did not give any reasons for why the two would not also have been liable as aiders and abettors of the Safeguards Rule violations. The cofounders settled with the SEC for $25,000 apiece.[180]

170. *See* Securities Exchange Act of 1934 § 17, 15 U.S.C. § 78q (2012); 17 C.F.R. § 240.17a-4 (2017); Craig Scott Capital, LLC, Exchange Act Release No. 77595, 2016 WL 1444441 (Apr. 12, 2016).

171. *Craig Scott Capital*, Exchange Act Release No. 77595, 2016 WL 1444441, at *2.

172. *Id.*

173. *Id.*

174. *Id.* *2–3.

175. *Id.* at *4.

176. *Id.* at *4–5.

177. *Id.* at *5.

178. Presumably, the chief compliance officer would have been in charge of ensuring CSC was complying with all security laws and regulations. Thus, it is unclear why the SEC was concerned that CSC's safeguard policies did not specify a designated officer in charge of compliance. *See id.* at *4. Even more interesting is why the chief compliance officer was not liable as an aider and abettor for CSC's failure to comply with the Safeguards Rule. *See id.* at *4–5.

179. *Id.* at *5.

180. *Id.* at *6.

h. Morgan Stanley Smith Barney

The SEC's most recent Safeguards Rule proceeding was also its largest. In 2016, the SEC brought an action against Morgan Stanley, ultimately settling for one million dollars.[181] A data breach was the trigger for the SEC's investigation against Morgan Stanley. Unlike all the other Safeguards Rule cases, however, the outside attackers did not steal the data directly from Morgan Stanley. Rather, they stole the data from an employee who had in turn stolen the data from Morgan Stanley.[182]

The employee's job was to assist one of Morgan Stanley's registered financial advisors.[183] As part of his position, he was supposed to have access to only his financial advisor's customer records through Morgan Stanley's firm intranet system. However, he discovered several flaws in the system that allowed him to access all customer records, regardless of the managing advisor.[184] Over the course of a year, he conducted thousands of searches.[185] He transferred the records he took to his own personal server, purportedly so he could study market trends and learn how advisors managed client funds.[186] Even though he did not intend to use the data in a harmful way, an outside attacker broke into his server and stole the data.[187]

Morgan Stanley discovered the breach during a routine Internet sweep, finding that the attacker had posted some of the data online along with an offer to sell the rest.[188] Morgan Stanley immediately took steps to fix the problem. It began by identifying the individual employee as the source of the breach. It then determined which records he had taken and notified the potentially affected customers—

181. Morgan Stanley Smith Barney LLC, Exchange Act Release No. 78021, Investment Advisers Act Release No. 4415, 2016 WL 3181325 (June 8, 2016). Interestingly, the FTC also considered bringing an action against Morgan Stanley, ultimately deciding to leave the matter alone. Letter from Maneesha Mithal, Assoc. Dir., FTC Div. of Privacy & Identity Prot., to Lisa J. Sotto, Partner, Hunton & Williams LLP (Aug. 10, 2015), https://www.ftc.gov/system/files/documents/closing_letters/nid/150810morganstanleycltr.pdf [https://perma.unl.edu/R8VU-JFWM]. While the FTC's letter seems to indicate that Morgan Stanley handled its data breach appropriately, it also points out that the letter "should not be construed as a determination that a violation [of section 5] did not occur." *Id.*

182. *Morgan Stanley*, Exchange Act Release No. 78021, Investment Advisers Act Release No. 4415, 2016 WL 3181325, at *2.

183. *Id.* at *3. The employee later also became a financial advisor—before Morgan Stanley discovered the data breach. *Id.* However, the distinction is unimportant for purposes of the SEC settlement.

184. *Id.*

185. *Id.* at *4.

186. *Id.*; Sentencing Memorandum, *supra* note 2.

187. *Morgan Stanley*, Exchange Act Release No. 78021, Investment Advisers Act Release No. 4415, 2016 WL 3181325, at *4.

188. *Id.*

all 730,000 of them.[189] It also took steps to remove the data from the Internet, though the settlement order does not describe those efforts in detail. Finally, Morgan Stanley notified law enforcement and other authorities of the breach.[190]

The SEC brought an enforcement action against Morgan Stanley for violations of the Safeguards Rule. Morgan Stanley certainly had policies in place regarding safeguarding private customer information, but the SEC found the policies did not meet the "reasonably designed" standard of the Safeguards Rule in two aspects. First, although Morgan Stanley did have policies and procedures in place designed to limit employee access to records, its staff did not properly design the electronic systems that should have prevented the CSA's actions.[191] Second, Morgan Stanley's employees failed to conduct appropriate audits on its intranet system—audits that presumably would have caught the problem earlier.[192] The settlement order does not specify whether Morgan Stanley's written policies required such testing.

In fact, the settlement order does not give clear examples of how Morgan Stanley's policies and procedures failed the *reasonably designed* standard.[193] The SEC's only discussion of the actual Safeguards Rule takes place in three short paragraphs—an unfortunate omission, considering the size of the settlement and Morgan Stanley's apparent good-faith attempts to protect customer data by adopting written policies and procedures. The only reasoning the SEC gave for its decision was:

> Although [Morgan Stanley] *had adopted written policies and procedures* relating to the protection of customer [data], those policies and procedures were not reasonably designed to safeguard its customers' [data] as required by the Safeguards Rule. For example, [Morgan Stanley's] written policies and procedures failed to adequately address certain key administrative, technical and physical safeguards, such as: reasonably designed and operating authorization modules for the [intranet] Portal[s] to restrict employee access to only the confidential customer data as to which such employees had a legitimate business need; auditing and/or testing of the effectiveness of such authorization modules; and monitoring and analyzing of employee access to and use of the Portals.[194]

B. Other Statutes and Regulations

Clearly, the SEC's primary data-security tool is the Safeguards Rule. However, the SEC has given guidance on other rules it might

189. *See id.* at *1, *4.
190. *Id.* at *4. The order never specifically says whether Morgan Stanley contacted the SEC, saying only that Morgan Stanley notified "law enforcement and other authorities." *Id.*
191. *Id.* at *3.
192. *Id.*
193. *See id.* at *5.
194. *Id.* (emphasis added).

use in proceedings against investment intermediaries who suffer data breaches or otherwise fail to safeguard customer data. These rules divide into two categories: (1) those rules that the SEC has merely threatened to use and (2) those rules that the SEC has actually used. In general, the rules the SEC has threatened to use would be applicable in situations where the investment intermediary was a victim of a data breach, whereas the rules it has actually used apply only in situations where the investment intermediary was actively doing something wrongful.

1. Statutes and Regulations the SEC Has Threatened to Use

The SEC's primary guidance on data-breach liability is a guidance update from 2015.[195] In this guidance update, the SEC cited three rules (in addition to the Safeguards Rule) that might impose liability on investment intermediaries who suffer data breaches: (1) the Investment Company/Adviser Compliance Rules, (2) the Identity Theft Red Flags Rules in Regulation S-P, and (3) rules pertaining to trade executions under the Investment Company Act.[196] To date, the SEC has not actually used any of these statutes or regulations in a Safeguards Rule proceeding.

The Compliance Rules only apply to registered investment companies and investment advisers; they do not apply to registered broker-dealers.[197] These provisions are Rule 38a-1 under the Investment Company Act and Rule 206(4)-7 under the Investment Advisers Act.[198] While the text of the two rules differs (Rule 38a-1 imposes stricter standards), the rules generally impose the same three basic requirements for investment companies and advisers: they must (1) adopt policies and procedures to comply with all federal securities laws, (2) perform annual reviews of their policies, and (3) designate chief compliance officers who will be in charge of implementing the policies.[199] These requirements act essentially as a second version of the Safeguards Rule—at least in the data-security context. An invest-

195. CYBERSECURITY GUIDANCE, *supra* note 14.

196. *Id.* at 4–5. The SEC also hinted that data breaches might lead to insider trading violations or other fraudulent activity. However, the limit of employer insider-trading liability is beyond the scope of this Comment. *See generally* John P. Anderson, *When Does Corporate Criminal Liability for Insider Trading Make Sense?*, CLS BLUE SKY BLOG (Jan. 24, 2017), http://clsbluesky.law.columbia.edu/2017/01/24/when-does-corporate-criminal-liability-for-insider-trading-make-sense/#_edn1 [https://perma.unl.edu/RRW7-8EKD]. Suffice it to say, investment intermediaries probably would not be liable for insider trading done by outside attackers. *See* CYBERSECURITY GUIDANCE, *supra* note 14, at 5 n.9 (describing liability for breaches "from insiders"); Anderson, *supra*.

197. *See* CYBERSECURITY GUIDANCE, *supra* note 14, at 4 n.7.

198. 17 C.F.R. §§ 270.38a-1, 275.206(4)-7 (2017).

199. *See* §§ 270.38a-1, 275.206(4)-7.

ment company or adviser that fails to adopt policies under the Safeguards Rule would also presumably violate the Compliance Rules, given that they require adoption of policies to comply with all securities laws (including the Safeguards Rule).

The Identity Theft Red Flags Rules came from a joint rule released by the SEC and the Commodity Futures Trading Commission.[200] The rule imposes two general requirements on all investment intermediaries. First, they must periodically determine whether they have certain types of customer accounts.[201] These customer accounts include "any . . . account . . . for which there is a reasonably foreseeable risk to customers . . . from identity theft."[202] Most types of customer accounts likely fall under this broad definition (especially if the investment intermediary maintains records of financial information, social security numbers, etc.). Second, investment intermediaries that maintain these covered customer accounts must establish a plan "designed to detect, prevent, and mitigate" identity theft arising from opening or maintaining such accounts.[203] Just like the Compliance Rules,[204] the Identify Theft Red Flags Rules are effectively a second version of the Safeguards Rule, requiring investment intermediaries to monitor for and try to prevent breaches.

Finally, rules relating to the execution of trades under the Investment Company Act only apply to registered investment companies, not to investment advisers or broker-dealers.[205] These rules work together to govern redemptions of investment-company shares. For example, if an investment company issues redeemable shares and the holder of those shares requests a redemption, section 22(e) requires the investment company to honor the redemption within seven days.[206] Rule 22c-1 requires the investment company to redeem the shares at their value as it was calculated on the date of the redemp-

200. Identity Theft Red Flags Rules, 78 Fed. Reg. 23,637 (Apr. 19, 2013) (codified in scattered parts of 17 C.F.R.).

201. 17 C.F.R. § 248.201(c) (2017).

202. § 248.201(b)(3)(ii).

203. § 248.201(d). The text of the rule actually says the plan must be "designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account"—note the lack of the word "maintain." *Id.* However, an investment intermediary could not "open" an "existing account," so presumably the SEC intended for this rule to cover accounts even after opening them.

204. *See supra* notes 197–99 and accompanying text.

205. *See* Investment Company Act of 1940 § 22(e), 15 U.S.C. § 80a-22(e) (2012) ("[n]o registered investment company"); 17 C.F.R. § 270.22c-1(a) (2017) ("[n]o registered investment company").

206. § 80a-22(e). A few exceptions to the seven-day requirement exist, such as for times when the SEC determines an "emergency exists" that would prevent redemptions. § 80a-22(e)(2). However, the SEC has never promulgated rules defining when it would deem an emergency to exist. *See* 17 C.F.R. pt. 270 (2017); *see also infra* subsection VI.B.3. (describing how the SEC can use its authority to

tion request.[207] A data breach might implicate both rules if it prevented the investment company from calculating the daily share price or otherwise redeeming the shares within seven days.[208]

2. Statutes and Regulations the SEC Has Actually Used

In its Safeguards Rule proceedings, the SEC has used a few rules other than the Safeguards Rule itself. First, Rule 10 of Regulation S-P forbids investment intermediaries from disclosing private client data to unaffiliated third parties without obtaining customer authorization.[209] Second, section 17 of the Exchange Act and Rule 17a-4 work together to require broker-dealers to preserve certain records relating to their business.[210]

Rule 10 is unlikely to apply in any situation in which an investment intermediary is only a passive victim of a data breach. The text of the rule prohibits investment intermediaries from *disclosing* private client information to third parties—a characterization that implies the investment intermediary must take an action (either transferring the data or permitting its transfer).[211] The SEC's adopting release for Regulation S-P also suggests that violations of Rule 10 require action on the part of the investment intermediary, describing how the act after which it was modeled "prohibits a financial institution . . . from *sharing* nonpublic personal information."[212] In any case, the SEC seems to have adopted this approach. In its four cases involving data breaches without any active transfers of data by the investment intermediary, the SEC did not use Rule 10.[213]

On the other hand, the recordkeeping requirements for broker-dealers might pose a threat in a data-breach situation. In the context of Safeguards Rule proceedings, the SEC has only used these rules once. In its *Craig Scott Capital* decision, the SEC imposed a fine on

define when an emergency exists to protect innocent victims of breaches from section 22 liability).

207. § 270.22c-1(a).

208. CYBERSECURITY GUIDANCE, *supra* note 14, at 5 n.11.

209. 17 C.F.R. § 248.10 (2017).

210. Securities Exchange Act of 1934 § 17, 15 U.S.C. § 78q (2012); 17 C.F.R. § 240.17a-4 (2017); *see also* 17 C.F.R. § 240.17a-3 (2017) (establishing the actual records broker-dealers must keep).

211. *See* § 248.10.

212. Privacy of Consumer Financial Information (Regulation S-P), 65 Fed. Reg. 40,333, 40,351 (June 29, 2000) (codified at 17 C.F.R. pt. 248) (emphasis added).

213. Morgan Stanley Smith Barney LLC, Exchange Act Release No. 78021, Investment Advisers Act Release No. 4415, 2016 WL 3181325 (June 8, 2016); R.T. Jones Capital Equities Mgmt., Inc., Investment Advisers Act Release No. 4204, 2015 WL 5560846 (Sept. 22, 2015); Commonwealth Equity Servs., LLP, Exchange Act Release No. 60733, Investment Advisers Act Release No. 2929, 2009 WL 3100577 (Sept. 29, 2009); LPL Fin. Corp., Exchange Act Release No. 58515, Investment Advisers Act Release No. 2775, 2008 WL 4179915 (Sept. 11, 2008).

the investment intermediary because its employees were actively trying to avoid the recordkeeping requirements by sending records to nonfirm e-mail addresses.[214] However, a broker-dealer theoretically could violate the recordkeeping requirements if it were to lose all of its records in a data breach (e.g., a hacker deletes all of the records on a broker's server). Although the SEC has not used these requirements like this in the past, it could do so in the future.[215]

V. REASONS TO REJECT THE STATUS QUO

In some ways, the SEC has done some things very differently than the FTC. However, the reality is that the SEC's approach and the FTC's approach are not as different as one might believe. The SEC has taken the FTC's general approach—using enforcement actions to develop a quasi-common law regarding data-security best practices—but on a much smaller scale. In a sense, the SEC has created a regulatory scheme that everybody, both opponents and proponents of the FTC's approach, can find objectionable. Opponents of the FTC's approach would disagree with the SEC's choice of strategy, while proponents would disagree with how the SEC is executing its strategy.

A. Reasons Opponents of the FTC's Approach Would Reject the SEC's Approach

Opponents of the FTC's approach can find several things about the SEC's approach to like. First, Congress gave the SEC explicit authority to regulate the data-security practices of investment intermediaries.[216] Thus, the SEC's actions have a legitimacy that the FTC's do not, considering the FTC's general approach has been to stretch its authority under section 5 to police the data security practices of every business in the country.[217] Additionally, the SEC's statutory mandate is relatively narrow, giving it authority only to regulate the data-security practices of investment intermediaries—firms that realize they must comply with the SEC's mandates and pay attention to its releases.

214. Craig Scott Capital, LLC, Exchange Act Release No. 77595, 2016 WL 1444441, at *1 (Apr. 22, 2016).

215. However, the SEC did not raise the possibility in its 2015 cybersecurity guidance. *See* CYBERSECURITY GUIDANCE, *supra* note 14. Thus, whether the SEC would use these recordkeeping rules in this manner is debatable. The answer might depend on whether the broker-dealer was making an honest effort to protect the records from outside attackers.

216. Gramm–Leach–Bliley Act of 1999, Pub. L. No. 106-102 § 501, 113 Stat. 1338 (codified at 15 U.S.C. § 6801 (2012)).

217. *Cf.* Hurwitz, *supra* note 32, at 1005 ("The FTC's [data security enforcement] efforts would affect every business handling electronic consumer data in the country—effectively, that is, every business in the country. If ever there were a case for expecting Congress to speak clearly, this would be it.").

However, these considerations do not change the fact that the SEC is ultimately using the FTC's basic approach to data security, and it is causing several of the same problems the FTC is. One problem is that some of the fairness concerns still apply—investment intermediaries are not receiving fair notice of what actions might lead to massive fines. For example, consider the *LPL Financial* decision.[218] The SEC assessed a $275,000 fine against LPL as part of its settlement agreement because "LPL failed to take *immediate* corrective action" when it discovered the vulnerabilities in its online system.[219]

But in a sense, LPL did take "immediate corrective action." In fact, it was handling the situation in a way that many, if not most, businesses would. After its internal audit team discovered the vulnerabilities, they reported their findings to the chief information officer, telling him that proposed fixes to the existing online system would cost more than $500,000.[220] The chief information officer then took the findings to other members of LPL's senior management, who in turn presented it to the firm's executive risk committee.[221] Within one month of the executive risk committee hearing about the findings, it had formed "a separate committee to evaluate and implement security" fixes for the systems.[222] In short, LPL's employees were handling the situation like many businesses would handle a $500,000 problem—examining the pros and cons of various approaches and trying to determine a solution that would fit their needs.

In fact, one notable government entity seemed to endorse the very approach that LPL took: the SEC itself back when it first proposed the Safeguards Rule.[223] In that release, the SEC stated, "We have not prescribed specific policies or procedures that financial institutions must adopt. Rather, we believe it more appropriate for each institution to tailor its policies and procedures to its own systems of information gathering and transfer and the needs of its customers."[224] LPL's risk

218. *LPL Fin.*, Exchange Act Release No. 58515, Investment Advisers Act Release No. 2775, 2008 WL 4179915, at *4.

219. *Id.* (emphasis added).

220. *Id.*

221. *Id.*

222. *Id.*

223. *See* Privacy of Consumer Financial Information (Regulation S-P), 65 Fed. Reg. 12,354, 12,365 (Mar. 8, 2000).

224. *Id.* Additionally, it is worth noting that the SEC has reiterated its support for letting investment intermediaries develop their own unique solutions to data security. CYBERSECURITY GUIDANCE, *supra* note 14, at 3 n.3 (giving suggestions for addressing data-security issues but emphasizing that "[t]hese suggested measures are not intended to be comprehensive and other measures *may be better suited* depending on the operations of a particular [investment intermediary]" (emphasis added)); Luis A. Aguilar, Comm'r, Sec. & Exch. Comm'n, Remarks at the SINET Innovation Summit (June 25, 2015) [hereinafter Aguilar Remarks], https://www.sec.gov/news/speech/threefold-cord-challenge-of-cyber-crime.html

committee could have taken any number of approaches. It might have decided to adopt the $500,000 proposed fixes, or it might have decided to go in an entirely different direction, abandoning its then-current online platform in favor of a new system. Further, even if LPL had "immediately" rubber stamped the proposed fixes, it still might have suffered the breach it did; nothing guarantees that proposed "fixes" will solve anything (even when they cost more than $500,000). LPL's risk committee deserved a fair chance to consider multiple possible solutions. In any case, LPL was handling things the way the SEC seemingly wanted it to—considering its unique risks and business situation and trying to handle the problem in a practical manner.[225] For its trouble, it wound up paying the second-largest fine the SEC has assessed in any of its Safeguards Rule actions.[226]

The *LPL Financial* decision raises an issue that is present in any after-the-breach determination of whether a given policy or procedure was reasonable: the risk of hindsight bias.[227] "Tertiary hindsight" is a problem in which a person who has learned the outcome of a situation "faults others for failing to predict it."[228] This happens because people who know the results of a situation tend to see those results as having always been inevitable.[229] While studies have sought to find a way to reduce hindsight bias's effects, the fact remains that data-breach victims in Safeguards Rule proceedings face a risk of prejudice.[230] When the SEC investigates an investment intermediary that has suffered a data breach, the SEC knows that any policies or procedures the intermediary had adopted ultimately proved to be inadequate at preventing the breach. However, that does not necessarily mean the investment intermediary did not reasonably design its policies and procedures; data breaches are almost inevitable, even for businesses with outstanding data-security practices.[231] Still, SEC investigators are almost certain to give too much credence to the breach's occur-

---

[https://perma.unl.edu/G552-R2MG] (describing how the SEC's approach to rulemaking recognizes that "entities must develop procedures that are tailored to their unique risks").

225. *See* Privacy of Consumer Financial Information (Regulation S-P), 65 Fed. Reg. at 12,365.

226. *See infra* Table 1 (providing an overview of all the SEC's Safeguards Rule actions, organized by the size of the assessed penalty).

227. *See* Maggie Wittlin, *Hindsight Evidence*, 116 COLUM. L. REV. 1323, 1359–62 (2016) (describing the problems associated with hindsight bias).

228. *Id.* at 1359–60.

229. *Id.* at 1359.

230. *See id.* at 1362–63 (describing the prejudice that hindsight bias causes in trials generally and ways of trying to ameliorate the issue).

231. *See supra* Part II.

rence when assessing whether the investment intermediary had implemented adequate data-security practices.[232]

In a closely related problem, when the SEC brings an enforcement action under the Safeguards Rule, it is acting as both a judge and a prosecutor.[233] While a judge in a court has incentives to thoughtfully consider both sides of a case, the SEC has incentives to selectively bring cases it can easily win so it can further its views on data security.[234] Given that investment intermediaries generally have not attempted to contest the SEC's actions,[235] the SEC has been able to shape the law of data security unilaterally based on its views of what policies and procedures are "reasonable."[236] Further, the lack of adversity from investment intermediaries has allowed the SEC to release numerous opinions that are overbroad and lack clear explanation aside from the conclusion that the investment intermediary must have done something wrong.

Take for example the *GunnAllen Financial* settlement orders.[237] Part of the SEC's complaint against the three employees was that they used a flash drive to transport customer data.[238] As the SEC described it, taking data on the flash drive put it "at *substantial* risk of unauthorized access and misuse."[239] Ignoring the wrongful nature of

232. *See* Wittlin, *supra* note 227, at 1359–62. In a way, the hindsight-bias problem might also explain why the SEC does not provide much reasoning in its decisions. *See generally infra* notes 253–58 and accompanying text. In the SEC's view, the occurrence of a breach might make the investment intermediary's alleged violations of the Safeguards Rule self-evident.

233. Hurwitz, *supra* note 32, at 984.

234. *See id.*

235. Only two actions have gone before an ALJ, and the defendant deserved to lose in both situations. J.P. Turner's failure was that it did not adopt *any* Safeguards Rule policies or procedures. *See supra* subsection IV.A.2.c. NEXT Financial's main failures were its unauthorized disclosures of customer data; the Safeguards Rule violation was not a major part of the order. *See supra* subsection IV.A.2.a.

236. *See* Hurwitz, *supra* note 32, at 984.

237. *See supra* subsection IV.A.2.e.

238. *See* Frederick O. Kraus, Exchange Act Release No. 64221, 2011 WL 1325567, at *5 (Apr. 7, 2011).

239. *Id.* (emphasis added); *see also* David C. Levine, Exchange Act Release No. 64222, 2011 WL 1325568, at *5 (Apr. 7, 2011) ("[H]e placed customer information at risk of unauthorized access and misuse when he knowingly downloaded [it] . . . to a personal thumb drive that he physically took from the firm."). Granted, part of the SEC's concern might have been the "personal" nature of the flash drive. Presumably, this means Levine actually owned the drive, rather than it belonging to GunnAllen. However, the SEC never explains the distinction nor does it explain why it believed a personal drive would create more risk than any other drive (if that were in fact what it believed). A personal drive might have a virus on it that the firm could not protect against, but that would be a reason for not using personal drives in *any* circumstances, not just when transferring data. Of course, this is all speculation, given that the SEC never actually explained why it expressly used the word *personal* to describe the drive. In its orders, the SEC seemed more concerned with the mere *taking* of the data—its use of the word

the data transfer in the *GunnAllen* actions (the employees did not have customer authorization to give the data to the new employer), what principle should a reader take from the SEC's order? Was the SEC suggesting that flash drives are inappropriate and unsecure tools for transferring data from one firm to another? If so, why? Is the risk of a person misplacing a flash drive greater than the risk of an outside attacker breaking into an online transfer system (such as e-mail)? If flash drives are unacceptable, what tools should investment intermediaries use to transfer data?

Alternatively, the SEC's decision might have had less to do with the *means* of transporting the customer data and more with the *wrongfulness* of the transfer itself. However, this view is unsatisfying for a few reasons. First, the SEC already has a regulation to police unauthorized transfers of private customer data—Rule 10 of Regulation S-P.[240] Second, it seems like a stretch to say that *wrongfully* taking data on a flash drive is any riskier than *rightfully* taking data on the same drive. If the GunnAllen employees had gotten customer authorization to take the data, would the SEC still feel the use of the flash drive put the data "at substantial risk of unauthorized access and misuse"?[241] The SEC might have argued that a person who wrongfully takes data is also the type of person who would be less careful with it in general—but if the SEC was in fact taking that position, it should have offered and explained it in the opinion.

Regardless, the orders are what they are—overbroad decisions with very little explanation and unclear principles. Investment intermediaries attempting to comply with the Safeguards Rule ultimately play a sort of reasonableness roulette, hoping that the SEC will not second-guess their policies and procedures. In short, merely doing what the FTC is doing—albeit doing less of it—is not a good approach.

B. Reasons Proponents of the FTC's Approach Would Reject the SEC's Approach

Proponents of the FTC's approach to data security have one main suggestion for the FTC: they think the FTC should expand its role by bringing more actions against companies.[242] Bearing in mind that the

personal seems designed to make the GunnAllen employees' actions seem worse than they arguably were. In any case, this uncertainty only bolsters the argument that the SEC should give better reasoning in its orders.

240. 17 C.F.R. § 248.10 (2017).

241. *Kraus*, Exchange Act Release No. 64222, 2011 WL 1325567, at *5.

242. *See* Security Law Professors Brief, *supra* note 50, at 2–3; *Scope and Potential*, *supra* note 34, at 2266. Professors Hartzog and Solove also recommend the FTC "seek milder punishments . . . for companies that have done most things right and have made a good faith attempt at compliance." *Scope and Potential*, *supra* note 34, at 2297. Thus, they might also object to some of the SEC's harsher pun-

FTC has already brought dozens of data-security actions,[243] these proponents of the FTC's approach likely would be disappointed in the SEC's comparatively small number of actions and its lack of clear guidance in the actions it has brought.

Certainly, investment intermediaries can distill some principles from the SEC's decisions, some of which are the same as the principles that Professors Solove and Hartzog found with respect to FTC actions.[244] For example, the *Morgan Stanley* action suggests that "[f]ail[ing] to test the security of a . . . process" and "[f]ail[ing] to implement procedures to control access to information" are inadequate practices.[245] The *Commonwealth Equity* action indicates that "[f]ail[ing] to implement cheap, easy-to-use, or common industry security practices," such as installing antivirus software, is an inadequate practice.[246] Several of the SEC's decisions stand for the obvious proposition that failing to adopt any policies or procedures is a violation of the Safeguards Rule.[247]

However, the problem with the SEC's decisions, to the extent it is trying to copy the FTC's strategy of creating the "functional equivalent of common law," is that the SEC has not released enough of them.[248] Thus far, the SEC has released only eleven Safeguards Rule decisions.[249] Of those eleven, only three have happened since 2012.[250] Part of the argument for why the FTC's use of adjudications is appropriate is that "data security changes too quickly and is far too dependent upon context to be reduced to a one-size-fits-all checklist."[251] Thus, if the SEC wants to use adjudication to shape the law of data

---

ishments, such as the one-million-dollar fine it imposed in the *Morgan Stanley* decision.

243. *See* Hurwitz, *supra* note 32, at 957 (describing how the FTC had "brought over 50 enforcement actions" as of 2015).

244. *See Common Law of Privacy*, *supra* note 37, at 651–55.

245. *Id.* at 652–53; *see* Morgan Stanley Smith Barney LLC, Exchange Act Release No. 78021, Investment Advisers Act Release No. 4415, 2016 WL 3181325, at *2–3 (June 8, 2016).

246. *Common Law of Privacy*, *supra* note 37, at 653; *see* Commonwealth Equity Servs., LLP, Exchange Act Release No. 60733, Investment Advisers Act Release No. 2929, 2009 WL 3100577, at *4 (Sept. 29, 2009).

247. *See, e.g.*, R.T. Jones Capital Equities Mgmt., Inc., Investment Advisers Act Release No. 4204, 2015 WL 5560846 (Sept. 22, 2015).

248. *Cf. Common Law of Privacy*, *supra* note 37, at 619 (describing the FTC's actions as being "in many respects the functional equivalent of common law").

249. *See supra* subsection IV.A.2.

250. *Morgan Stanley*, Exchange Act Release No. 78021, Investment Advisers Act Release No. 4415, 2016 WL 3181325; Craig Scott Capital, LLC, Exchange Act Release No. 77595, 2016 WL 1444441 (Apr. 12, 2016); *R.T. Jones*, Investment Advisers Act Release No. 4204, 2015 WL 5560846.

251. *Scope and Potential*, *supra* note 34, at 2259.

security, it arguably needs to bring more actions and it needs to keep its decisions current to match changes in technology.[252]

Beyond that, proponents of the FTC's approach likely would want the SEC to give better reasoning in its actions. Professors Solove and Harzog describe in their article how "[t]hose [people] involved with helping businesses comply with privacy law . . . parse and analyze the FTC's settlement agreements, reports, and activities as if they were pronouncements by the Chairman of the Federal Reserve."[253] Assuming readers parse the SEC's data-security settlements in this manner, they likely will not find the type of guidance they seek. Although the SEC's orders do reveal some general principles,[254] they often do not describe these principles in enough detail to help future investment intermediaries with planning.[255]

For example, consider the *Morgan Stanley* action.[256] The SEC, in the course of assessing a one-million-dollar fine, spent only three paragraphs describing the ways in which Morgan Stanley failed to meet the Safeguards Rule's requirements. Further, only one of those three paragraphs arguably contained anything close to actual reasoning:

> Although [Morgan Stanley] had adopted written policies and procedures relating to the protection of customer [data], those policies and procedures were not reasonably designed to safeguard its customers' [data] as required by the Safeguards Rule. For example, [Morgan Stanley's] written policies and procedures failed to adequately address certain key administrative, technical and physical safeguards, such as: reasonably designed and operating authorization modules for the [intranet] Portal[s] to restrict employee access to only the confidential customer data as to which such employees had a legitimate business need; auditing and/or testing of the effectiveness of such authorization modules; and monitoring and analyzing of employee access to and use of the Portals.[257]

Now imagine if, instead of merely providing its conclusions, the SEC had given a fuller explanation of how Morgan Stanley's policies and procedures failed to satisfy its obligations under the Safeguards Rule:

> The Commission does not dispute that Morgan Stanley did in fact have policies and procedures as required by the Safeguards Rule. However, despite

252. *But see infra* section VII.B. (arguing that the SEC should *not* use this approach).
253. *Common Law of Privacy*, *supra* note 37, at 585.
254. *See supra* notes 244–47 and accompanying text.
255. *See supra* section V.A.
256. Morgan Stanley Smith Barney LLC, Exchange Act Release No. 78021, Investment Advisers Act Release No. 4415, 2016 WL 3181325 (June 8, 2016).
257. *Id.* at *5. The first of the three paragraphs only describes the general requirements found in the text of the Safeguards Rule. *Id.* The third paragraph says, "As a result of the conduct described above, [Morgan Stanley] willfully violated [the Safeguards Rule], which requires every broker-dealer and investment adviser registered with the Commission to adopt written policies and procedures that are reasonably designed to safeguard customer records and information." *Id.*

> its efforts, Morgan Stanley did not reasonably design its policies and procedures to protect private customer data. First, Morgan Stanley did not have adequate policies and procedures for limiting employee access to sensitive data. Firms today are more aware than ever of the threat that employees pose to sensitive data. For a large firm, especially one with millions of customer records and billions of dollars in annual revenue such as Morgan Stanley, protecting against employee mischief with numerous policies and procedures is both obvious and imperative.
>
> Second, Morgan Stanley's policies and procedures failed to adequately address its auditing processes for making sure that its internal systems did not have security flaws. Although its internal technology department was conducting periodic reviews, the procedures they were following should have caught an issue posing as much risk as the one the employee exploited. The employee's unauthorized access took place over the course of an entire year. During this time, Morgan Stanley's technology staff apparently did not notice a single red flag. Furthermore, the exploit itself was present in the system for at least as long as the employee was using it. An internal auditing procedure that misses such glaringly obvious security flaws is, simply put, not "reasonably designed."
>
> Considering the obviousness of the flaws, the number of inadequate policies and procedures, the length of time over which the data thefts occurred, the number of records put at risk, Morgan Stanley's size and ability to implement quality policies and procedures, and Morgan Stanley's knowledge of its obligations under the Safeguards Rule, the Commission finds that Morgan Stanley willfully violated the Safeguards Rule.[258]

In short, if the SEC is trying to adopt the FTC's data-security strategy, it is failing. Its few decisions do not give the clarity that others have found in the FTC's decisions,[259] and it has not brought enough actions to show investment intermediaries that it intends to aggressively police the data-security realm.[260]

---

258. This model discussion is based on the reasoning the SEC seemed to get at in its decision. The factual conclusions are debatable. Ideally, the explanation should have been even longer and more detailed than this model discussion, describing some of the policies and procedures Morgan Stanley had for limiting employee access to sensitive data and conducting internal audits. Regrettably, neither the SEC's order nor any other publicly available documents describe what specific policies and procedures Morgan Stanley had in place. In any event, an order written like this would give readers clearer guidance on the issues they should consider in developing their own policies and procedures.

259. *Cf. Common Law of Privacy*, *supra* note 37, at 651–55 (giving a list of the principles the authors found embodied in the FTC's decisions).

260. *See* Security Law Professors Brief, *supra* note 50, at 9–12 (describing the results of a survey indicating that companies take seriously the threat of FTC actions because they know the FTC uses its ability to police data-security practices liberally). *See generally* Bamberger & Mulligan, *supra* note 48 (describing how the "emergence of the FTC as a privacy regulator," among other developments in the market, has led companies to take data security more seriously than they have in the past).

VI. A THREE-PART PROPOSAL FOR ACHIEVING THE SEC'S DATA-SECURITY GOALS

Although the SEC must reject its current approach, its broad authority over investment intermediaries and their data-security practices gives it quite a bit of leeway to creatively solve its data-security dilemma.[261] The SEC's ultimate goal is—as it always has been—to encourage investment intermediaries to take data security seriously while still affording them freedom to tailor solutions to their own unique needs.[262] The SEC can accomplish this goal by (1) amending the Safeguards Rule, (2) amending some of its other rules, and (3) adopting a new enforcement approach.

A. Amendments to the Safeguards Rule

The SEC should begin addressing data-security matters by amending the Safeguards Rule. Subsection VI.A.1. offers the new version of the Safeguards Rule as the SEC should adopt it. Subsections VI.A.2. through VI.A.6. describe the key changes the proposed rule would make to the existing rule.

1. Text of the Proposed Regulation

(a) **Requirement.** Every investment intermediary must in good faith consider and adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. When developing these policies, the investment intermediary should seek to:

  (1) Ensure the security and confidentiality of customer records and information;

  (2) Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and

  (3) Protect against the unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

(b) **Duty to Update.** Every investment intermediary must adopt as part of its written policies and procedures a plan, designed in good faith, for keeping its adopted policies and procedures described in subsection (a) current (including the plan described in this subsection).

(c) **Recordkeeping.** Every investment intermediary must keep records regarding how it has developed its written policies and procedures described in subsections (a) and (b). These records must include:

261. *See* Gramm–Leach–Bliley Act of 1999, Pub. L. No. 106-102 § 501(b), 113 Stat. 1338 (codified at 15 U.S.C. § 6801(b) (2012)).

262. *See generally* Disposal of Consumer Report Information, 69 Fed. Reg. 71,321 (Dec. 8, 2004) (codified at 17 C.F.R. § 248.30); Privacy of Consumer Financial Information (Regulation S-P), 65 Fed. Reg. 40,333 (June 29, 2000) (codified at 17 C.F.R. pt. 248).

(1) In the case of a rejected policy or procedure, a brief description of the considered policy or procedure and a detailed description of the reasons for rejecting its adoption;

(2) In the case of an adopted policy or procedure (including amendments to or revocations of existing policies or procedures):

(i) A brief description of the policy or procedure, both as proposed and as adopted;

(ii) A detailed description of the reasons for accepting adoption of the final policy or procedure, including explanations of any changes from the policy or procedure as it was originally proposed; and

(iii) A description of the plan for implementing the policy or procedure; and

(3) In the case of all considered policies and procedures, whether adopted or rejected, a description of the process by which the decision to adopt or reject was made. This description shall include, at a minimum:

(i) A description of any investigations into the costs and benefits of the considered policy or procedure;

(ii) A description of any person or persons involved in the decision to accept or reject the considered policy or procedure (including persons whose involvement was limited to gathering and presenting information to the ultimate decision makers); and

(iii) The time spent on any considered policy or procedure.

Every investment intermediary must keep these records for a period no shorter than five years. In the case of a record relating to a currently adopted policy or procedure, the investment intermediary must keep the record for as long as the policy or procedure is in effect (including earlier versions of current policies or procedures and any considered revocations or amendments to current policies or procedures). An investment intermediary that fails to maintain these records will be in violation of this section.

(d) **Burden of Proof.** In any civil action or case brought by the SEC under this section, the investment intermediary shall have the burden of proving it acted in good faith. In any criminal action for an alleged willful violation of this section, the Department of Justice shall have the burden of proving the investment intermediary did not act in good faith.

(e) **Definitions.** For purpose of this section, the following definitions apply:

(1) **Adopt.** The term "adopt" means to put the policy or procedure into writing, implement it, and keep it current.

(2) **Consider.** The term "consider" means to examine a proposed policy or procedure and, after assessing its advantages and disadvantages in good faith, either accept and adopt it or reject it.

(3) **Good Faith.** The term "good faith" means a state of mind consisting of honesty in belief or purpose and faithfulness to the goal of protecting customer data and privacy.[263]

(4) **Investment Intermediary.** The term "investment intermediary" means any broker, dealer, investment company, or investment adviser as those terms are defined in 17 C.F.R. § 248.3.

263. *See Good Faith*, BLACK'S LAW DICTIONARY (10th ed. 2014).

2. Good Faith Obligation

The most important change the proposed rule would make is that it would replace the "reasonably designed" standard from the current Safeguards Rule with a "good faith" standard. Scholars that have written about data security and the FTC's enforcement actions tend to agree that a firm's good faith efforts at providing data security should be a factor in determining its potential liability.[264] This new rule would make that idea explicit, eliminating any after-the-fact determinations about whether an investment intermediary's policies and procedures were "reasonable" and instead shifting the focus to whether the investment intermediary was making an honest attempt to develop good policies and procedures.

Acting in good faith would be an absolute defense to any civil or criminal liability the SEC or Department of Justice might try to impose under the Safeguards Rule. For example, picture an investment intermediary that declines to purchase antivirus software for its systems because it decides the Windows Defender software that comes standard on every Microsoft operating system is sufficient. Although the SEC might disagree with the substance of the investment intermediary's decision, as long as the investment intermediary could show it reached that decision in good faith, considering the costs and benefits of purchasing commercial antivirus software, the SEC could not punish it under the Safeguards Rule.

Making this change would have several positive results. First, and most importantly, it would promote the type of compliance the SEC wants by clarifying the requirements investment intermediaries must meet. Rather than placing the emphasis on developing policies that the SEC will later find reasonable, the emphasis will shift to "encouraging firms to sit down, think about, and develop their policies."[265] As the SEC has indicated numerous times in the past, the best data-security solution is one in which individual investment intermediaries have incentives to develop policies tailored to their own unique risks and situations.[266] The proposed good faith requirement gives investment intermediaries that incentive by affording them the freedom to consider and adopt policies and procedures without worrying about the SEC second-guessing them.[267]

264. *See, e.g.*, *Scope and Potential*, *supra* note 34, at 2297 ("One thing the FTC could do is to seek milder punishments and shorter auditing periods for companies that have done most things right and have made a good faith attempt at compliance."); *cf.* Hurwitz, *supra* note 32, at 1016 (proposing a system that would be similar to a good faith defense in FTC proceedings: "encouraging firms to develop and disclose data security policies" and then requiring them to live up to those policies).

265. Hurwitz, *supra* note 32, at 1016.

266. *See supra* note 224.

267. *See* Wittlin, *supra* note 227, at 1359–62 (describing the problems associated with hindsight bias).

Additionally, moving to a good faith standard will almost immediately solve most of the unfairness concerns raised by the SEC's current approach. One point bears repeating: data-security breaches are nearly inevitable.[268] Modern businesses and organizations face threats from all directions, and they cannot possibly predict every attack they will encounter. Even the federal government itself has been the victim of numerous data breaches.[269] In fact, one of the most infamous data breaches involved a breach of one of the most secure government agencies: Edward Snowden's theft of highly classified data from the NSA.[270] In other words, breaches happen. Thus, the fairest possible regulatory scheme is one that examines not whether an investment intermediary suffered a breach but whether it made good faith efforts in trying to prevent the breach.

Further, eliminating the "reasonably designed" standard in favor of a good faith standard will actually make the SEC's enforcement efforts easier. It seems counterintuitive: the risk of a good faith standard is that an investment intermediary can throw poorly designed policies together and later lie about the time and thought it put into them. However, this risk is not as serious as it seems for a few reasons. First, subsection (d) of the proposed rule places the burden in civil actions on the investment intermediary to prove it acted in good faith.[271] This alleviates the SEC's burden in these cases by preventing it from having to prove what the investment intermediary's employees were thinking when they adopted (or rejected) a given policy or procedure.

Second, the rule as proposed comes with a strict recordkeeping requirement. Subsection VI.A.4. explains the details of this requirement

---

268. *See supra* Part II.

269. *See, e.g.*, Julie Hirschfeld Davis, *Hacking of Government Computers Exposed 21.5 Million People*, N.Y. TIMES, July 10, 2015, at A1, https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html; Nir Kshetri, *Why the IRS Was Hacked Again and What the Feds Can Do About It*, U.S. NEWS & WORLD REP. (Feb. 16, 2016), https://www.usnews.com/news/articles/2016-02-16/why-the-irs-was-hacked-again-and-what-the-feds-can-do-about-it [https://perma.unl.edu/8S2R-38VB]; Darlene Storm, *List of Hacked Government Agencies Grows: State Department, White House, NOAA & USPS*, COMPUTERWORLD (Nov. 17, 2014), http://www.computerworld.com/article/2848779/list-of-hacked-government-agencies-grows-state-department-white-house-noaa-and-usps.html [https://perma.unl.edu/V8VU-44TS]. Moreover, the SEC itself recently became the victim of a high-profile data breach. *See* Chris Isidore, *Why the SEC Hack Is a Really Big Deal*, CNN MONEY (Sept. 21, 2017), money.cnn.com/2017/09/21/news/sec-edgar-hack/index.html [https://perma.unl.edu/N5ZL-9A7A]

270. Dustin Volz, *How Did Snowden Steal Millions of Documents? He Had Help*, DEFENSE ONE (Feb. 13, 2014), http://www.defenseone.com/technology/2014/02/snowden-had-help/78830 [https://perma.unl.edu/6E22-V3GR].

271. Given the higher stakes and increased fairness concerns at issue in criminal actions, the proposed rule places the burden of proof on the Department of Justice to disprove that the investment intermediary was acting in good faith.

further, but the main point is that an investment intermediary must keep records of all policies and procedures it considers.[272] The investment intermediary also must describe, in detail, the reasons for ultimately accepting or rejecting those considered policies or procedures.[273] Thus, SEC regulators will have an abundance of evidence. They can examine the reasoning the investment intermediary gives in its records, and they can even look at the number of policies or procedures the investment intermediary has considered. If an investment intermediary has only ever considered a few policies or procedures, the SEC can point to that fact as evidence the firm is not acting in good faith.

One potential counterargument against the good faith standard is that it merely replaces one uncertain standard with another. Determining whether a given policy or procedure is reasonable is a facts-and-circumstances question, just like determining whether an investment intermediary is acting in good faith. However, the uncertainties presented by the reasonableness and good faith standards are very different. Some uncertainty is inevitable in the field of data security.[274] The proposed rule shifts that uncertainty from a highly technical area (determining the reasonableness of data-security policies and procedures) to one that most people can understand, especially given that the proposed rule defines good faith.[275]

Another possible counterargument is that the SEC should police the substance of investment intermediaries' data-security policies and procedures because any data breach—even one against a firm acting in good faith—hurts customers by exposing them to the risk of theft.[276] But when customers try to sue in the aftermath of data breaches, they often lose because of difficulties in proving actual damages; the mere risk of future harm often is not enough, nor is emo-

272. Importantly, the SEC regulators themselves can make recommendations to investment intermediaries about policies and procedures they should consider. *See infra* section VI.C.

273. *See infra* subsection VI.A.4.

274. *Cf. Scope and Potential*, *supra* note 34, at 2259 ("Yet data security changes too quickly and is far too dependent upon context to be reduced to a one-size-fits-all checklist."); Hurwitz, *supra* note 32, at 998 (describing the difficulty in "formulat[ing] specific rules ex ante" for "fast-moving areas, such as . . . data security").

275. *See infra* subsection VI.A.5.

276. *See generally* ANN CAVOUKIAN, A DISCUSSION PAPER ON PRIVACY EXTERNALITIES, SECURITY BREACH NOTIFICATION AND THE ROLE OF INDEPENDENT OVERSIGHT 4–5 (2009), https://www.ipc.on.ca/wp-content/uploads/Resources/privacy_externalities.pdf [https://perma.unl.edu/37DG-TJH8] (describing the negative externalities, such as loss of privacy, that result from data breaches). The author of this Comment wishes to thank Professor Gus Hurwitz of the University of Nebraska College of Law for raising this counterargument during a discussion with the author.

tional harm that purportedly results from a breach.[277] An independent government agency such as the SEC can enforce data-security standards where individual litigants cannot.[278] Moving to the good faith standard arguably would reduce the SEC's ability to protect customers from poorly designed policies and procedures.

However, the proposed Safeguards Rule actually does give the SEC quite a bit of ability to regulate investment intermediaries' policies and procedures. As described further in section VI.C., SEC regulators can recommend policies or procedures to investment intermediaries. Investment intermediaries that do not consider these recommended policies or procedures will not be acting in good faith and thus will be liable under the Safeguards Rule. Importantly, the purpose of the Safeguards Rule is not to allow the SEC to punish victims of data breaches; it is to promote positive data-security practices and encourage firms to keep their customers' data safe. As the SEC has noted repeatedly, investment intermediaries are in the best position to assess their own unique risks and develop their own defenses.[279] The proposed Safeguards Rule, along with a more vigorous enforcement approach by the SEC,[280] would promote this goal better than after-the-breach prosecutions about reasonableness by empowering investment intermediaries to take creative approaches to data security while giving the SEC a clearer mandate.[281]

3. Duty to Update

Subsection (b) of the proposed Safeguards Rule contains the only policy/procedure that an investment intermediary must adopt: a plan for keeping all of its Safeguards Rule policies and procedures current. As others have noted, "Cybersecurity is not a problem to be solved, but [is instead] a continuous threat that demands constant attention."[282] Thus, investment intermediaries must consider policies and procedures designed to maintain their data-security policies and procedures in light of changing technologies and threats.

277. Hooker & Pill, *supra* note 33, at 36–37; *see also* Danielle Citron, *Some Good News for Data Breach Victims, for a Change*, FORBES (July 21, 2015), https://www.forbes.com/sites/daniellecitron/2015/07/21/some-good-news-for-data-breach-victims-for-a-change/#4071ba69469a [https://perma.unl.edu/4PTU-972L] (describing the difficulty in recovering damages as a plaintiff in a data-breach lawsuit).

278. *See generally* CAVOUKIAN, *supra* note 276, at 11–13.

279. *See, e.g.*, CYBERSECURITY GUIDANCE, *supra* note 14; Aguilar Remarks, *supra* note 224.

280. *See infra* section VI.C.

281. If anything, this counterargument against the proposed Safeguards Rule might be a good argument for making it easier for data-breach victims to show actual damages in private lawsuits. However, that is a very different issue than whether we should allow the SEC to impose punitive fines on investment intermediaries based on an unpredictable and ever-changing "reasonably designed" standard.

282. Martin, *supra* note 21; *accord* Aguilar Remarks, *supra* note 224.

As with all policies and procedures, investment intermediaries must only design their updating plan in good faith according to their own risks and situations. This approach allows the SEC to stay faithful to its stated goal of allowing investment intermediaries to develop their own policies and procedures.[283] Alternative approaches, such as requiring investment intermediaries to reconsider their policies and procedures every couple of months or every time some triggering event (e.g., a data breach) occurs, would be contrary to the SEC's goals and would risk incentivizing firms to focus on compliance rather than security. For example, if the SEC required investment intermediaries to examine their policies and procedures once every three months, firms likely would *only* check their policies every three months regardless of whether they should check more often.[284]

4. Recordkeeping Requirement

As briefly described before,[285] the proposed Safeguards Rule will avoid some of the concerns in determining whether an investment intermediary has considered policies and procedures in good faith by imposing a strict recordkeeping requirement. Subsection (c) begins by dictating the records investment intermediaries must keep. If an investment intermediary considers a policy but ultimately does not adopt it, the firm must keep a brief description of the considered policy and a *detailed* description of the reasons for rejecting it.

If the investment intermediary adopts a considered policy—including amendments to or revocations of an existing policy—paragraph (c)(2) requires it to include three main pieces of information in its records. First, the records must briefly describe the policy or procedure, both as it was originally proposed and as it was finally adopted. Second, the records must describe in detail the reasons for adopting the final version of the policy or procedure. Third, the records must explain how the investment intermediary plans to implement the policy or procedure. Simply saying something like "our firm policy is to restrict employee access to records" is not enough; the investment intermediary must give ways it will actually restrict access.

Additionally, investment intermediaries must include in *all* records the processes by which they ultimately adopted or rejected the considered policies and procedures. Paragraph (c)(3) establishes at least three parts of this requirement, each of which will allow the SEC

283. *See* Privacy of Consumer Financial Information (Regulation S-P), 65 Fed. Reg. 12,354, 12,365 (Mar. 8, 2000) ("We have not prescribed specific policies or procedures that financial institutions must adopt. Rather, we believe it is more appropriate for each institution to tailor its policies and procedures to its own systems of information gathering and transfer and the needs of its customers.").

284. *See infra* section VII.A. (describing the "checkbox compliance" problem).

285. *See supra* text accompanying notes 272–73.

to determine whether the firm has acted in good faith. First, these records must include any information gathering the investment intermediary undertook when considering the proposed policies and procedures. For example, if an investment intermediary had an employee perform a cost–benefit analysis of a proposed policy, it would include a description of that in the records. The proposed rule also incentivizes investment intermediaries to perform these types of analyses for its considered policies—the investment intermediary will include any analyses in its records, which it in turn can use to demonstrate good faith. Second, these records must include a description of all people involved in making the decision to accept or reject a considered policy or procedure. Third, these records must include a description of the time the investment intermediary's employees spent considering the policy or procedure.

Finally, subsection (c) requires that investment intermediaries keep all Safeguards Rule records for a minimum of five years. Five years would strike a balance between the SEC's interest in seeing records and investment intermediaries' interests in minimizing recordkeeping costs. Seeing a five-year period of records will give the SEC a good idea of whether an investment intermediary is acting in good faith generally when considering its policies. However, an exception to the five-year rule is that an investment intermediary must keep records relating to a policy or procedure it currently has in effect for as long as the policy or procedure is in effect. Otherwise, the SEC might not be able to examine the reasoning behind these policies and procedures to see how they have evolved over time.

In addition to helping the SEC handle investigations of specific investment intermediaries, the recordkeeping requirement will have another major benefit: it will provide the SEC with a vast amount of information on how investment intermediaries are thinking about data security. The SEC, as part of its data-security efforts, has shown interest in understanding the policies and procedures that investment intermediaries actually adopt. For example, in 2014 the SEC hosted a roundtable in which SEC commissioners and staff met with industry representatives, soliciting feedback about the SEC's data-security approaches.[286] Additionally, in 2015 the SEC's Office of Compliance Inspections and Examinations sent out a survey to more than one hundred investment intermediaries, seeking feedback on their approaches to data security and their concerns with modern threats and SEC regulations.[287] The SEC uses this information to create its re-

286. *Cybersecurity Roundtable*, SEC. & EXCHANGE COMMISSION, https://www.sec.gov/spotlight/cybersecurity-roundtable.shtml [https://perma.unl.edu/9CNC-Q497] (last modified May 11, 2016).

287. OCIE SWEEP SUMMARY, *supra* note 68. In 2017, the Office of Compliance Inspections and Examinations released findings from a follow-up data-security sweep.

leases and provide guidance to investment intermediaries about data-security practices.[288] By establishing a recordkeeping requirement in the Safeguards Rule, the SEC would gain access to all the information it could want about how investment intermediaries handle their data-security practices.[289]

The recordkeeping requirement might be subject to criticism because of the costs it imposes on investment intermediaries. It is true that creating and maintaining records is not free. However, the proposed Safeguards Rule would not cause any large or undue burdens. The records themselves are hardly complex; investment intermediaries essentially must specify what they decided, how they made those decisions, and why they made those decisions. Investment intermediaries already must have policies and procedures under the current version of the Safeguards Rule—the proposed rule just requires them to create a minimal paper trail.[290] Additionally, any burden will lessen with time, as firms become more accustomed to keeping the Safeguards Rule's required records and develop standard forms for doing so.

A second possible counterargument is that investment intermediaries could always forge files after the fact to make it seem as though they were acting in good faith all along. But the risk of fraud is not a reason to reject the proposed rule any more than it is a reason to reject the current version of the Safeguards Rule. After all, an investment intermediary could always create records in response to notice of an SEC investigation under the current system.[291] Further, an investment intermediary cannot commit this type of fraud in response to a

---

OCIE 2017 UPDATE, *supra* note 68. The OCIE included with its findings a brief list of policies and procedures for investment intermediaries to consider. *Id.* at 4–5.

288. *See, e.g.*, CYBERSECURITY GUIDANCE, *supra* note 14.

289. *See infra* section VI.C. (describing how the SEC can use this information to provide guidance to investment intermediaries).

290. For example, if an investment intermediary considers and ultimately rejects a policy, its record will only need to say something along the lines of:

> We considered [policy] and ultimately rejected it because [detailed reasons]. Our I.T. department analyzed the change; their findings are included with this record (along with the names of the I.T. staff who assisted in the analysis). Once they reached their conclusions, they submitted their findings to the chief compliance officer, [name]. He accepted their reasoning and rejected the policy. This process lasted over the course of one week.

291. If an investment intermediary maintains its Safeguards Rule records in electronic format, the SEC can analyze the files' metadata to determine when the firm made them, when it last edited them, etc. *See generally* Philip J. Favro, *A New Frontier in Electronic Discovery: Preserving and Obtaining Metadata*, 13 B.U. J. SCI. & TECH. L. 1 (2007). This might be an argument for requiring investment intermediaries to maintain their files electronically, rather than in physical (paper) form. However, that discussion is beyond the scope of this Comment, given its conclusion that the risk of fraud is already minimal.

suggested policy or procedure that comes directly from the SEC. If the SEC, in the course of auditing an investment intermediary, suggests a policy or procedure, it will not have to worry about when the firm considered the proposal; it will only care about the firm's decision and reasoning. In short, the specter of fraud is no greater under the proposed rule than it is under any rule, including the current Safeguards Rule.

5. Definitions

Subsection (e) of the proposed Safeguards Rule defines a few terms. First, it clarifies that "adopting" a policy or procedure means putting it into writing, implementing it, and keeping it current. Second, subsection (e) defines "consider" as "examin[ing] a proposed policy or procedure and, after assessing its advantages and disadvantages in good faith, either accept[ing] it or reject[ing] it." This helps elaborate on the process investment intermediaries must follow when analyzing possible policies or procedures. Third, it defines "investment intermediary" to include every broker, dealer, investment company, and investment adviser. This helps shorten the text of the rule's main requirements, thus making the rule clearer and more concise.

Most importantly, paragraph (e)(3) defines "good faith" as "a state of mind consisting of honesty in belief or purpose and faithfulness to the goal of protecting customer data and privacy."[292] Courts have struggled with defining good faith in many instances.[293] However, affirmatively defining good faith in the rule itself will alleviate some of this problem, giving courts a standard by which they can judge a defendant's conduct. Further, this definition applies perfectly to the goal the SEC wants to achieve, which is to "encourag[e] firms to sit down, think about, and develop their policies."[294] Of course, this definition will still leave some uncertainty—determining whether a firm acted

292. This definition is based on the definition of "good faith" found in the tenth edition of *Black's Law Dictionary*. *See Good Faith*, BLACK'S LAW DICTIONARY (10th ed. 2014).

293. *See, e.g.*, Andrew S. Gold, *A Decision Theory Approach to the Business Judgment Rule: Reflections on* Disney*, Good Faith, and Judicial Uncertainty*, 66 MD. L. REV. 398, 399–400 (2007) (describing the difficulties in defining the corporate duty of good faith before the Supreme Court of Delaware reached its decision in *In re Walt Disney Co. Derivative Litigation*, 906 A.2d 27 (Del. 2006)); Alan D. Miller & Dr. Ronen Perry, *Good Faith Performance*, 98 IOWA L. REV. 689, 694 (2013) (describing good faith in the context of contract law, saying that "[d]espite the general acceptance and apparent importance of good-faith performance in the United States, courts and scholars have not been able to agree on the exact meaning of this concept").

294. Hurwitz, *supra* note 32, at 1016; *see also* CYBERSECURITY GUIDANCE, *supra* note 14 (recognizing that investment intermediaries face unique risks based on their specific situations).

in good faith depends on facts and circumstances. However, a point that bears repeating is that eliminating all uncertainty from data-security regulation is effectively impossible, given the complexity of the topic and the rapid evolution of technology and threats.[295] Rather, the goal should be to shift uncertainty away from a highly technical and constantly changing standard (the reasonableness of data-security policies and procedures) to one that people can understand.

6. Removal of the Current Subsection (b)

The final change is that the proposed rule would remove the current subsection (b) from the Safeguards Rule. The current subsection (b) deals with disposal of consumer-report information, as required by the Fair Credit Reporting Act.[296] In short, this rule does not need to be a part of the Safeguards Rule. This is not to say the SEC should eliminate the disposal rule. Rather, it should move the rule to a new section of the Code of Federal Regulations, possibly 17 C.F.R. § 248.31 (currently unused).

B. Application of the Safeguards Rule Amendments to Other Statutes and Regulations

Amending the Safeguards Rule is not enough. As described in section IV.B., the SEC has a number of regulations it can use in data-security cases. Taking a good faith approach under the Safeguards Rule would not accomplish its intended purpose if the SEC were able to force investment intermediaries to adopt "reasonably designed" policies and procedures under other provisions.[297] Fortunately, most of the SEC's other rules do not conflict with the proposed version of the Safeguards Rule.

1. Investment-Company and Investment-Adviser Compliance Rules

Both Rule 38a-1 under the Investment Company Act and Rule 206(4)-7 under the Investment Adviser Act require adoption and implementation of "written policies and procedures reasonably designed to prevent violation" of federal securities laws.[298] Fortunately, neither should create any problems for the proposed version of the Safeguards Rule. The Safeguards Rule requires implementation of specific types of policies and procedures—those designed to protect customer data.

295. *See supra* note 274 and accompanying text.
296. 17 C.F.R. § 248.30(b) (2017).
297. *See, e.g.*, 17 C.F.R. § 248.201(d)(2) (2017) (requiring all investment intermediaries to develop "*reasonable* policies and procedures to" prevent and catch identity theft (emphasis added)).
298. 17 C.F.R. §§ 270.38a-1, 275.206(4)-7 (2017).

In contrast, the Compliance Rules require only that investment companies and investment advisers adopt policies and procedures for complying with other securities rules. Thus, adopting data-security policies and procedures in good faith will satisfy these rules without regards to the substance of those policies and procedures.

2. Identity Theft Red Flags Rules

The Identity Theft Red Flags Rules pose the greatest issue of the SEC's other regulations, given their explicit requirement that all investment intermediaries must adopt "reasonable policies and procedures to" prevent and catch identity theft.[299] Unlike the Compliance Rules described in subsection VI.B.1., this requirement poses an issue because, like the Safeguards Rule, it involves policies and procedures specifically designed to handle data-security issues. While drafting a new version of the Identify Theft Red Flags Rules is beyond the scope of this Comment, the SEC must amend them in a similar way to the proposed Safeguards Rule, replacing the reasonableness language with a good faith standard.

3. Investment-Company Redemption Rules

The SEC does not need to change Rule 22c-1 under the Investment Company Act, which only establishes the price at which investment companies must honor redemption requests by shareholders.[300] This requirement does not have any inconsistencies with the proposed Safeguards Rule. Additionally, section 22(e) does not conflict with the Safeguards Rule, requiring only that investment companies generally honor certain types of redemptions within seven days of the request.[301]

However, the SEC could adopt one new regulation that could help a data-breach victim avoid section 22(e) liability. If a data breach prevents an investment company from honoring a redemption request within seven days, the SEC has said that the investment company "may be in violation of section 22(e)."[302] However, section 22(e) also says that the seven-day redemption requirement does not apply "for any period during which an emergency exists."[303] Section 22(e) does not define "emergency exists"; it gives the SEC authority to determine via rule or regulation when it will deem an emergency to exist.[304] Therefore, the SEC could adopt a regulation deeming an emergency to

299. § 248.201(d)(2).
300. 17 C.F.R. § 270.22c-1(a) (2017).
301. *See* Investment Company Act of 1940 § 22(e), 15 U.S.C. § 80a-22(e) (2012).
302. CYBERSECURITY GUIDANCE, *supra* note 14, at 5 n.11.
303. § 80a-22(e)(2).
304. *Id.*; § 80a-22(e)(i). The SEC has never promulgated rules clarifying when it would deem an emergency to exist. *See* 17 C.F.R. pt. 270 (2017).

exist in any situation in which an investment intermediary has complied with its obligations under the Safeguards Rule but has still suffered a data breach preventing it from redeeming shares.

4. Rule 10 of Regulation S-P

The SEC does not need to make any changes to Rule 10 of Regulation S-P, at least given the way the SEC is currently using it.[305] The SEC has never used Rule 10 against an investment intermediary that was only a passive victim of a data breach. In fact, Rule 10 covers a very different issue than the Safeguards Rule. While the Safeguards Rule's purpose is to make investment intermediaries think about their data-security practices, Rule 10 is about preventing investment intermediaries from actively disclosing data to nonaffiliated third parties without customer permission.[306] Thus, the rules already should not conflict.

5. Broker-Dealer Recordkeeping Rules

As described in subsection IV.B.2., broker-dealers must keep certain business records.[307] Theoretically, a broker-dealer could violate these requirements if it lost all of its records in a data breach. One solution is to trust the SEC to use its prosecutorial discretion to not punish victims of data breaches who made good faith efforts to protect their systems. Thus far, this has not been a problem—the only time the SEC used these recordkeeping rules in a Safeguards Rule proceeding was because the investment intermediary was actively attempting to avoid its recordkeeping obligations.[308] Further, the proposed version of the Safeguards Rule might handle any potential issues by encouraging investment intermediaries to consider policies and procedures for backing up important records.

C. Enforcement of the New Safeguards Rule

Subsections VI.A.2. and VI.A.4. already described how the new Safeguards Rule would actually make the SEC's job easier by shifting the burden of proof and giving it ample information via the recordkeeping requirement. In many ways, the SEC's enforcement strategy would not have to change. The main difference is that rather than looking for investment intermediaries with unreasonable policies and

305. *See* 17 C.F.R. § 248.10 (2017); *supra* subsection IV.B.2.
306. *See* Privacy of Consumer Financial Information (Regulation S-P), 65 Fed. Reg. 40,333, 40,334 (June 29, 2000).
307. *See* Securities Exchange Act of 1934 § 17, 15 U.S.C. § 78q (2012); 17 C.F.R. § 17a-4 (2017).
308. *See* Craig Scott Capital, LLC, Exchange Act Release No. 77595, 2016 WL 1444441, at *1 (Apr. 12, 2016).

procedures, it would look for investment intermediaries seemingly not complying with the Safeguards Rule in good faith. Additionally, the SEC could take the opportunity under the new rule to be more aggressive in its enforcement efforts.[309] "Aggressive" in this context does not mean the SEC would be trying to punish investment intermediaries who seem to have complied in good faith; it only means that the SEC would be vigilant in examining investment intermediaries' records.

However, one additional part of the SEC's enforcement authority requires discussion: its ability to propose policies and procedures to investment intermediaries. As the SEC investigates various investment intermediaries, it undoubtedly will find gaps in some firms' policies and procedures. Not all of these gaps will, considered alone, be evidence of bad faith. Investment intermediaries will inevitably overlook some threats or possibilities, given how quickly technology changes and the nearly limitless number of ways in which an attacker can exploit a data-security system.[310] When the SEC finds these possible issues, it can propose policies and procedures the investment intermediaries should consider.[311] Doing so will put the burden on the investment intermediary to actually consider the proposed policy or procedure in good faith; a firm that fails to consider one of these proposed policies or procedures would not be acting in good faith.

For example, if the SEC had investigated Morgan Stanley in the months before the breach, it might have found the issues regarding how Morgan Stanley was conducting its internal data-security audits.[312] These issues alone likely would not have shown that Morgan Stanley was acting in bad faith. In fact, Morgan Stanley had policies and procedures in place and, given its size and reputation, had almost certainly considered them in good faith.[313] Nevertheless, it overlooked something, and that something ultimately led to the theft of thousands of customer records.[314] Had the SEC, in one of its routine investigations, discovered the problems, it could have alerted Morgan Stanley to the risks and prompted Morgan Stanley to consider various possible fixes.

An investment intermediary could always reject an SEC proposal—its only requirement would be considering the proposal in good faith. Thus, the SEC could work closely with investment in-

309. *See infra* section VII.B.
310. *See supra* Part II.
311. The Office of Compliance Inspections and Examinations did this in its 2017 data-security release. *See* OCIE 2017 UPDATE, *supra* note 68, at 4–5. The proposed Safeguards Rule would take these suggestions and give them real power by requiring investment intermediaries to consider them in good faith.
312. *See* Morgan Stanley Smith Barney LLC, Exchange Act Release No. 78021, Investment Advisers Act Release No. 4415, 2016 WL 3181325, at *5 (June 8, 2016).
313. *See id.*
314. *Id.* at *2.

termediaries to build a system of public–private collaboration in developing and implementing quality data-security practices.[315] The new Safeguards Rule, when combined with the SEC's enforcement authority, would result in the best possible outcome for all interested parties. Investment intermediaries would gain the certainty of knowing they would not face punitive fines in after-the-breach adjudications regarding the reasonableness of their policies, the SEC would gain the ability to promote data security while collecting information about industry practices, and customers would gain the safety that comes with better data security.

VII. POSSIBILITIES THE SEC SHOULD REJECT

The three-part solution offered in Part VI of this Comment would yield the best possible data-security outcomes. It would take the focus away from after-the-fact determinations of whether a given policy or procedure was reasonable, shifting it instead to encouraging investment intermediaries to pursue data-security solutions in an honest and faithful manner. However, the SEC might consider other possible solutions to its data-security dilemma. The SEC should reject other possibilities that various academics have offered. None will help it achieve its goal of letting market participants analyze and develop their own policies and procedures while still enabling it to play a role in shaping data-security practices.

A. Establish a Checklist of Specific Data-Security Standards with Which Investment Intermediaries Must Comply

The first possible option the SEC might consider is adoption of clear substantive requirements under the Safeguards Rule with which investment intermediaries must comply. In other words, this possible "solution" is to abandon the overwhelming consensus on data security by encouraging firms to adopt checkbox-compliance mentalities.[316] The problem with checkbox compliance is that it diverts a firm's atten-

315. *See* Aguilar Remarks, *supra* note 224 (referring to statements by other government leaders about the importance of collaboration between the public and private sectors in data security issues); Jeh Johnson, Sec'y of Homeland Sec., Remarks at RSA Conference 2015 (Apr. 21, 2015), https://www.dhs.gov/news/2015/04/21/remarks-secretary-homeland-security-jeh-johnson-rsa-conference-2015 [https://perma.unl.edu/3X92-NE25] ("Cybersecurity must be a partnership between government and the private sector.").

316. *See, e.g.*, *Scope and Potential*, *supra* note 34, at 2259 ("Yet data security changes too quickly and is far too dependent upon context to be reduced to a one-size-fits-all checklist."); Hurwitz, *supra* note 32, at 998 (describing the difficulty in "formulat[ing] specific rules ex ante" for "fast-moving areas, such as . . . data security"); Aguilar Remarks, *supra* note 224 ("[E]ntities must develop procedures that are tailored to their unique risks."); Basani, *supra* note 15 ("The 'checkbox' mentality places too much emphasis on Compliance over Risk Management.").

tion away from creating data-security policies and procedures designed to meet its unique needs, instead focusing on achieving "wooden compliance with a checklist of practices that may reduce future liability risk, but do not advance enterprise security."[317]

The SEC, to its credit, has rejected this approach so far. Instead, the SEC has allowed investment intermediaries to develop their own solutions to data-security issues.[318] Although the category "investment intermediaries" only includes four types of entities—brokers, dealers, investment companies, and investment advisers—the principle of wanting unique solutions tailored to unique risks is the same. Different investment intermediaries have different systems for handling sensitive data. They interact with different software vendors, keep different types of records, work with different types of clients, have different net assets, etc. While they might be more similar in their business situations than, say, a car dealership and a university, their individual risks and needs are still unique. Trying to use a one-size-fits-all approach would ignore these realities, putting the SEC in the uncomfortable position of trying to create a rule that would somehow satisfy the data-security requirements of every investment intermediary.[319]

Further, even if the SEC could determine a perfect list of policies and procedures for investment intermediaries that would ensure data security, it would have trouble maintaining that list in a regulation. Data-security issues evolve quickly—technologies change and new threats arise constantly.[320] In contrast, the administrative rulemaking process does not move quickly, with new regulations and amendments to existing regulations sometimes taking years to pass.[321] This problem likely would be even more apparent in the data-security area, considering the difficulty in creating before-the-fact rules designed to protect customer information.[322] In sum, adopting specific requirements in a regulation would not help the SEC further its goal of en-

317. Archis A. Parasharami & Stephen Lilley, Wyndham*, Heartbleed, and the Pitfalls of Setting Cybersecurity Standards Through Litigation*, DATA SEC. L. REP. (2014), https://www.mayerbrown.com/files/News/97e0b26e-afbf-4522-85ab-4304a92d844d/Presentation/NewsAttachment/a75a9e2e-f126-4b39-a253-44788ef84463/Data%20Protection%20Law%20Reporter%20(Pitfalls%20of%20Setting%20Cybersecurity)%202014.pdf.

318. *See* Privacy of Consumer Financial Information (Regulation S-P), 65 Fed. Reg. 12,354, 12,365 (Mar. 8, 2000).

319. *Cf.* Aguilar Remarks, *supra* note 224 ("[E]ntities must develop procedures that are tailored to their unique risks.").

320. *See supra* Part II.

321. *See generally* Thomas O. McGarity, *Some Thoughts on "DeOssifying" the Rulemaking Process*, 41 DUKE L.J. 1385 (1992).

322. *See Scope and Potential*, *supra* note 34, at 2259.

couraging investment intermediaries to protect customer data; it would actually undermine that objective.[323]

B. Aggressively Enforce the Safeguards Rule as It Currently Exists

One reason that proponents of the FTC's approach to data security likely would object to the SEC's approach is the infrequency with which the SEC has brought its Safeguards Rule actions. Therefore, the SEC might consider being more aggressive in its enforcement of the current version of the Safeguards Rule. However, this approach would do nothing to solve the fairness concerns that stem from its current efforts.[324]

Additionally, adopting the proposed version of the Safeguards Rule would actually do more to further the FTC proponents' interests than merely enforcing the existing rule more frequently. First of all, the two options are not mutually exclusive; the SEC can adopt the new version of the Safeguards Rule *and* aggressively enforce it.[325] More importantly, proponents of the FTC's approach describe how its efforts "spur[ ] companies to hire information privacy and security specialists who then develop evolving best practices" in data security.[326] However, that is exactly what the new version of the Safeguards Rule is designed to do. Further, the proposed Safeguards Rule would do a better job of helping the SEC determine best practices by requiring that investment intermediaries keep detailed records of the policies and procedures they consider. In short, the propositions offered in Part VI, taken as a whole, would be a way of bridging the gap between opponents and proponents of what the FTC is doing, reducing the unfairness in the SEC's current approach while enabling it to strengthen its data-security regulation efforts.

C. Cease Regulating Data-Security Practices

Businesses, including investment intermediaries, have many reasons to take their data security seriously even in the absence of government regulation. Simply put, a data breach is an expensive event. A recent study by the Ponemon Institute, a private research center

323. For the reasons explored in this section, adopting a safe-harbor regulation would be equally ineffective at promoting good data-security policies and procedures. *But see* Jeff Kosseff, *Positive Cybersecurity Law: Creating a Consistent and Incentive-Based System*, 19 CHAP. L. REV. 401, 412–14 (2016) (arguing that the FTC should consider adopting a safe harbor).

324. *See supra* section V.A.

325. *See supra* section VI.C.

326. Security Law Professors Brief, *supra* note 50, at 2; *see also Scope and Potential*, *supra* note 34 (arguing that the FTC's efforts have led to better data security practices in the market).

that studies data security, found that a data breach can cause a company to lose millions of dollars.[327] A company that suffers a breach might have direct out-of-pocket costs, such as buying affected customers subscriptions to identity-theft monitoring services. But some of the most important costs are those that result from harm to the victim-company's reputation (e.g., losing customers who no longer trust the business to protect their data).[328]

Ignoring for a moment the fact that the Gramm–Leach–Bliley Act requires the SEC to regulate data-security standards,[329] one might conclude that market incentives already provide enough pressure for investment intermediaries to take data security seriously. However, while this is undoubtedly true in some cases, not every investment intermediary will be a "good actor." In fact, several of the SEC's Safeguards Rule actions have come against investment intermediaries that had no policies or procedures in place for safeguarding customer data.[330] In other words, market forces are not always sufficient to drive companies to give careful thought to their data-security practices. Given the harm that can result from a data breach—both to the company itself and to affected customers—the SEC is right to make investment intermediaries consider their policies and procedures.[331] The proposed Safeguards Rule strikes a balance, allowing the SEC to continue its work in promoting data security while shielding investment intermediaries from punitive fines when those intermediaries make good faith attempts to protect customer data.[332]

VIII. CONCLUSION

Despite this Comment's criticisms regarding the SEC's data-security efforts, one point is worth remembering: the SEC has done a com-

327. PONEMON INST., 2016 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS 2 (2016), https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN [https://perma.unl.edu/M9ZV-VN43].

328. *Id.* at 3.

329. Gramm–Leach–Bliley Act of 1999, Pub. L. No. 106-102 § 501(b), 113 Stat. 1338 (codified at 15 U.S.C. § 6801(b) (2012)) ("[E]ach agency or authority . . . *shall* establish appropriate standards . . . ." (emphasis added)).

330. *See, e.g.*, R.T. Jones Capital Equities Mgmt., Inc., Investment Advisers Act Release No. 4204, 2015 WL 5560846 (Sept. 22, 2015).

331. *See* PONEMON INST., *supra* note 327, at 2–3 (describing the costs incurred by businesses and customers in the wake of data breaches).

332. *Compare* Morgan Stanley Smith Barney LLC, Exchange Act Release No. 78021, Investment Advisers Release Act No. 4415, 2016 WL 3181325 (June 8, 2016) (the investment intermediary arguably did not deserve its fine because it had adopted Safeguards Rule policies and procedures and it was attempting to protect customer data in good faith, as evidenced by its compliance with authorities in the aftermath of the breach), *with* J.P. Turner & Co., LLC, 98 SEC Docket 1729, 2010 WL 2000509 (ALJ May 19, 2010) (the investment intermediary had no policies or procedures in place and thus clearly deserved a fine).

paratively good job handling the modern problem of consumer-data protection. Unlike the FTC, the SEC has made a conscientious effort to solicit public feedback and develop its authority through notice-and-comment rulemaking. Further, it has been mindful of the costs regulated investment intermediaries face. Rather than attempting to strong-arm them into adopting expensive and potentially unnecessary policies and procedures, the SEC has given them freedom to develop individualized solutions tailored to their own unique situations.

Work remains, but the SEC is in a perfect situation to build upon its successes while avoiding its past failures. By abandoning its current enforcement approach and adopting the rules and policies recommended in this Comment, the SEC can build the regulatory scheme for data security by which all others would be judged. These changes would not require much effort on the SEC's part and they would actually make its enforcement role easier. With the right mindset, the SEC can set the bar for public–private collaboration in the area of data security, developing a system that encourages innovation, responsibility, and fairness.

APPENDIX: SAFEGUARDS RULE PROCEEDINGS

The SEC has issued eleven orders involving violations of the Safeguards Rule. This appendix includes a table displaying an overview of the SEC's decision. Because subsection IV.A.2. of the text already describes the SEC's decisions in chronological order, this chart organizes them by penalty size. The decisions (organized chronologically, most recent first) are:

1. Morgan Stanley Smith Barney LLC, Exchange Act Release No. 78021, Investment Advisers Act Release No. 4415, 2016 WL 3181325 (June 8, 2016);
2. Craig Scott Capital, LLC, Exchange Act Release No. 77595, 2016 WL 1444441 (Apr. 12, 2016);
3. R.T. Jones Capital Equities Mgmt., Inc., Investment Advisers Act Release No. 4204, 2015 WL 5560846 (Sept. 22, 2015);
4. David C. Levine, Exchange Act Release No. 64222, 2011 WL 1325568 (Apr. 7, 2011);
5. Frederick O. Kraus, Exchange Act Release No. 64221, 2011 WL 1325567 (Apr. 7, 2011);
6. Marc A. Ellis, Exchange Act Release No. 64220, 2011 WL 1325566 (Apr. 7, 2011);[333]
7. J.P. Turner & Co., LLC, 98 SEC Docket 1729, 2010 WL 2000509 (ALJ May 19, 2010);
8. Commonwealth Equity Servs., LLP, Exchange Act Release No. 60733, Investment Advisers Act Release No. 2929, 2009 WL 3100577 (Sept. 29, 2009);
9. Stephen Cheryl Bauman, Exchange Act Release No. 60326, 2009 WL 2138437 (July 17, 2009);
10. LPL Fin. Corp., Exchange Act Release No. 58515, Investment Advisers Act Release No. 2775, 2008 WL 4179915 (Sept. 11, 2008);
11. NEXT Fin. Grp., Inc., 93 SEC Docket 1369, 2008 WL 2444775 (ALJ June 18, 2008).

333. David Levine, Frederick Kraus, and Marc Ellis were all part of GunnAllen Financial, Inc. GunnAllen had discontinued operations by the time the SEC issued the orders in the three proceedings, so there is no separate GunnAllen decision.

Table 1: Administrative Orders Organized by Penalty Size (Largest First)

Defendant	Year	Fine Amount	Actual Breach?[334]	Safeguards Violations	Other Violations	Other Information
Morgan Stanley	2016	$1,000,000	Yes, an employee stole data from the firm.	Had an exploit in its online data portals, enabling employees to access all customer files (not just those for their customers). Did not catch this error during audits, and did not carefully analyze employee access.	None	Intrusions occurred over the course of one year. Potentially compromised 730,000 accounts. Morgan Stanley quickly notified law enforcement, the SEC, and affected customers.
LPL Financial	2008	$275,000	Yes, an outside attacker breached the firm's defenses.	LPL did have written policies regarding client data. But: 1. No minimum password requirements; 2. No automatic password expiration; 3. Users could not	None	LPL had approximately 1,000,000 customer accounts. The attacker might have had access to 10,000 of them. The attacker placed unauthorized

334. In this context, "Actual Breach?" refers to whether somebody accessed or took confidential information *without authorization* (at least based on the facts available in the SEC proceedings). Thus, most of the "No" proceedings for this column involve situations in which management permitted an employee or multiple employees to remove data.

Defendant	Year	Fine Amount	Actual Breach?[334]	Safeguards Violations	Other Violations	Other Information
				set their own passwords; 4. No automatic lockout for failed login attempts; 5. Many employees had access to password lists; 6. User accounts took eight hours to log out automatically.		trades, but LPL's systems blocked most of them, and LPL reimbursed customers for any losses. The SEC's main concern seems to have been that LPL knew about the risk, but was moving too slowly to fix it.
NEXT Financial	2008	$125,000	No.	The Safeguards Rule violation appears to be mainly a tack-on charge, with the SEC saying the firm did not secure its client data because it allowed employees to take it to new employers when they left.	17 C.F.R. § 248.10 (sharing customer info without authorization).	The primary violation was of Rule 10 of Regulation S-P, dealing with obtaining customer consent before sharing data.
Craig Scott Capital	2016	$100,000 Two of CSC's employees also	No.	Did have written policies, but had five weaknesses:	Exch. Act. § 17; 17 C.F.R. § 240.17a-4	The primary violations appear to have been for

Defendant	Year	Fine Amount	Actual Breach?[334]	Safeguards Violations	Other Violations	Other Information
		faced fines, but their fines were solely for violations of Exch. Act § 17 (maintaining certain records).		1. Did not have a compliance supervisor; 2. Policies did not address eFaxes; 3. Policies had blank spaces; 4. Did not encrypt data; 5. Employees regularly violated the policies.	(failing to maintain certain records).	failure to keep certain records (faxes it received and sent via an eFax system). The SEC also censured two employees as part of its proceedings.
C'wealth Equity	2009	$100,000	Yes, an outside attacker breached the firm's defenses.	C'wealth Equity (CES) did have policies in place, and was attempting to comply with the Safeguards Rule. However, the policies did not mandate antivirus software, and IT services did not respond quickly to an employee's calls saying he had a computer virus.	None	CES had over 165,000 accounts. The intruder only got access to 368 of them. The intruder placed unauthorized trades, which CES caught and stopped (reimbursing customers for losses caused by the ones that went through). Additionally, CES quickly reported the incident to

Defendant	Year	Fine Amount	Actual Breach?[334]	Safeguards Violations	Other Violations	Other Information
						law enforcement, the SEC, and its affected customers.
R.T. Jones	2015	$75,000	Yes, an outside attacker breached the firm's defenses.	Did not have any written policies whatsoever regarding data security.	None	The attacker gained access to the information of more than 100,000 individuals. Although it did not have written policies in place, R.T. Jones quickly hired cybersecurity firms to assess the damage. Additionally, it informed all potentially affected individuals.
J.P. Turner	2010	$65,000	No.	J.P. Turner went years without having any policies. When it finally adopted policies, they were deficient. They merely	None	The SEC discovered the problem after seeing a news story about a J.P. Turner employee who left boxes containing

Defendant	Year	Fine Amount	Actual Breach?[334]	Safeguards Violations	Other Violations	Other Information
				quoted the Safeguards Rule and said the Acting Chief Compliance Officer would be in charge of adopting further policies. The ACCO (Stephen Bauman) never adopted any further policies.		thousands of customer records (including social security numbers and bank account numbers) on the curb outside of his house (for pickup by a trash company). Although it does not appear anybody stole the files, they sat on the curb for two weeks. The SEC argued for a higher penalty, but the ALJ capped the amount at $65,000, finding J.P. Turner did not act recklessly.
David Levine	2011	$20,000	No.	Levine was the GunnAllen (GA) employee who downloaded 16,000 client files to a flash drive to take to a new	17 C.F.R. §§ 248.7, .10 (sharing customer information without authorization).	For Levine and Krause, it seems as though the primary charges were for sharing customer information with

Defendant	Year	Fine Amount	Actual Breach?[334]	Safeguards Violations	Other Violations	Other Information
				employer (with Frederick Kraus's permission). He was a senior officer, so the SEC attributed some of GA's failures to him.		a new firm without permission. The SEC did point out that the thumb drive was not secure.
Frederick Kraus	2011	$20,000	No.	Kraus was president of GunnAllen while it was winding up business. As president, he failed to adopt policies regarding protection of customer information during the winding-up phase. Additionally, he permitted David Levine to download 16,000 customer files to a flash drive to take to another firm.	17 C.F.R. §§ 248.7, .10 (sharing customer information without authorization).	For Kraus and Levine, it seems as though the primary charges were for sharing customer information with a new firm without permission. The SEC did point out that the flash drive was not secure.
Marc Ellis	2011	$15,000	No.	Ellis was the Chief Compliance	None	Although three laptops containing

Defendant	Year	Fine Amount	Actual Breach?[334]	Safeguards Violations	Other Violations	Other Information
				Officer for GunnAllen (GA). GA only had weak written policies (barely one page long, and without much substance). Additionally, somebody stole three laptops containing customer data, but GA never followed up beyond reporting the thefts to police.		data (including social security numbers) of 1,120 clients (and employee login information) went missing, GA never alerted the clients. Because Ellis was in charge of compliance, the SEC attributed GA's faults to him.
Stephen Bauman	2009	$0	No.	Bauman was J.P. Turner's Acting Chief Compliance Officer and thus was in charge of making sure it complied with the Safeguards Rule.	None	Bauman's only penalty was that she had to cease and desist from violating the Safeguards Rule in the future. She was aware of the Safeguards Rule's existence while she was at J.P. Turner.