Dissenting Statement of Commissioner Noah Joshua Phillips and Commissioner Christine S. Wilson

Regulatory Review of Safeguards Rule
Matter No. P145407

March 5, 2019

Today the Commission seeks public comment on a notice of proposed rulemaking ("NPRM") to change the Standards for Safeguarding Customer Information ("Safeguards Rule" or "Rule") under the Gramm-Leach-Bliley Act ("GLBA"). Recent high-profile data breaches underscore the importance of effective data security, which is why we strongly support the Commission's renewed calls for federal data security legislation.[1] We also share this Administration's goal of reducing regulation and controlling compliance costs. Any new regulation, even regarding a critical issue like data security, must be handled with care to avoid stifling innovation or entrenching incumbents.

Congress mandated data security and privacy for financial institutions in the GLBA and, for the past two decades, it has been the Commission's responsibility to set forth the regulations implementing those requirements. The Rule as written provides direction to financial institutions on how to protect data security – importantly, while not being overly prescriptive – in an area where standards continuously evolve. The current proposal, however, trades flexibility for a more prescriptive approach, potentially handicapping smaller players or newer entrants.[2]

As part of our regular process of regulatory review, the Commission first sought comments on updating the Safeguards Rule in September 2016.[3] When asked about the need for more specific requirements, commenters generally asked to leave the Rule in place, and to avoid more prescriptive regulation. Privacy advocates and an association owned by the largest commercial banks sought more detailed requirements.[4] Based on that record, and the adoption of several new

---

[1] *See Oversight of the Federal Trade Commission: Hearing Before the Subcomm. on Consumer Protection, Product Safety, Insurance, and Data Security of the S. Comm. on Commerce, Science, and Transportation*, 115th Cong. 7 (2018) (statement of the Federal Trade Commission) ("The Commission continues to reiterate its longstanding bipartisan call for comprehensive data security legislation."); Federal Trade Commission Staff, Comment to the National Telecommunications and Information Administration on Developing the Administration's Approach to Consumer Privacy (Nov. 9, 2018), https://www.ftc.gov/policy/advocacy/advocacy-filings/2018/11/ftc-staff-comment-ntia-developing-administrations-approach.

[2] *See, e.g.*, William A. Brock & David S. Evans, The Economics of Regulatory Tiering, 16 RAND J. ECON. 398, 399 (1985) ("[I]mposing uniform regulatory requirements across all types of businesses has a disparate impact on smaller businesses because there are scale economies in regulatory compliance. Scale economies may arise because there are fixed costs of complying with regulations. Larger businesses can average these fixed costs over a larger quantity of output and thereby achieve a competitive advantage over their smaller rivals. [¶] There is evidence that scale economies in compliance are quite extensive for some regulatory requirements.") (citations omitted).

[3] Standards for Safeguarding Customer Information, 81 Fed. Reg. 61632 (Sept. 7, 2016) (to be codified at 16 C.F.R. pt. 314). Comments are posted at https://www.ftc.gov/policy/public-comments/2016/10/initiative-674. The Commission has assigned each comment a number.

[4] Electronic Privacy Information Center, Comment Letter #30 on the Standards for Safeguarding Customer Information (Nov. 7, 2016); The Clearing House Association LLC, Comment Letter #35 on the Standards for Safeguarding Customer Information (Nov. 21, 2016).

state laws and regulations regarding data security of financial institutions, the Commission today proposes the latter course.

This approach concerns us for several reasons. *First*, some of the specific proposals track shortcomings the Commission has identified in its data security enforcement cases and investigations. Not all of these shortcomings concern firms covered by the Safeguards Rule and, in any event, they may not represent a broader trend that warrants a regulatory response. Therefore, it may not be appropriate to mandate such prescriptive standards for all market participants. To the extent that the Commission thinks it is appropriate to elucidate the regulation's reasonable care requirements, we have tools at our disposal – including speeches, testimony, analyses to aid public comment, information about the factors the Commission considered when closing investigations, and reports. Commentary like this can help financial institutions weigh whether precautions are reasonable based on the risks associated with how they use, collect, and store data, without imposing a one-size-fits-all approach. The question to be answered here is whether the existing Safeguards Rule, which addresses the protection of financial information, is inadequate to that purpose. Also important is the question of how firms governed by the Rule operate relative to ones in sectors that are not so governed.

Second, the proposed regulations may be premature for two reasons. They are based in substantial part on regulations promulgated two years ago by the New York State Department of Financial Services.[5] We do not have data about the impact and efficacy of those regulations, so whether to adopt a version of them at the federal level and whether that version should be a floor for or should preempt state-level rules seem like questions worthy of more study. Right now, Congress and the Executive Branch, including the leadership of the Senate committee with jurisdiction over financial institutions, are discussing potential privacy and data security legislation.[6] The NPRM seeks comment on issues that are implicated in this debate, as well as issues not addressed in the New York rule, like data minimization/elimination and requiring a legitimate business justification for collecting data in the first instance. These topics in particular take us into a broader debate that belongs – and is being had – in Congress.

Third, the Safeguards Rule today is a flexible approach, appropriate to a company's size and complexity. This proposal would move us away from that approach. There are direct costs for enhanced precautions, but this record does not demonstrate that those costs will significantly reduce data security risks or significantly increase consumer benefits. The expansion of the Rule could create traps for the unwary, especially small and innovative businesses. Further, large incumbents can often absorb regulatory compliance costs more effectively than new entrants or smaller players, potentially decreasing competition.[7] The proposed precautions, either individually or in the aggregate, may constitute best practices for certain firms. But the proliferation of procedural, technical, and governance requirements may have the unintended consequence of diluting core data security measures undertaken pursuant to the existing Safeguards Rule.

---

[5] Cybersecurity Requirements for Financial Services Companies, 23 NYCRR 500, *et seq* (2016).
[6] Press Release, S. Comm. on Banking Housing, and Urban Affairs, *Crapo, Brown Invite Feedback on Data Privacy, Protection and Collection* (Feb 13, 2019), https://www.banking.senate.gov/newsroom/majority/crapo-brown-invite-feedback-on-data-privacy-protection-and-collection.
[7] *See* Brock and Evans, *supra* note 2.

Finally, the NPRM proposes that the Commission substitute its own judgment for a private firm's governance decisions, including but not limited to the appropriate level of board engagement,[8] hiring and training requirements,[9] and program accountability structures.[10] Data security is important, without doubt. In our enforcement and legislative advocacy, we focus a great deal on it. But take, for example, board engagement on data security. Whether and to what extent it should command the regular attention and personal liability of a company's board is precisely the kind of question firms are in a better position to evaluate than federal regulators. Other matters may be more important, including to the nation at large. A decade ago, our economy was brought low by what many view as improper risk assessment by financial institutions of their assets and liabilities. Maybe we want boards of financial institutions to spend more time assessing those risks. The point isn't that the answer is easy – the point is that we may not be the best qualified to supply it.

This is an NPRM, and the Commission is merely proposing new regulation and soliciting views on its impact. But we are also aware that the momentum behind an NPRM regularly results in the promulgation of new or revised rules. While the Commission is not making a final determination today, we are concerned that the specific suggestions herein will frame the debate so as to take the Commission in a direction that may be unwarranted (particularly given the prospect of legislation), and which may have negative repercussions. A review of the Safeguards Rule, especially in light of new legal developments, is warranted. But we should go where the evidence today leads us. We would strongly encourage those in industry, academia, and civil society with expertise in these areas to comment and provide evidence on this proposal.

For these reasons, we dissent.

[8] Standards for Safeguarding Customer Information (proposed Mar. 5, 2019) (16 C.F.R. pt. 314.4(i)) (requiring that Chief Information Security Officer ("CISO") report in writing, at least annually, to board of directors or equivalent about the overall status and material matters related to the information security program based on the assumption that "such reports will not be overly burdensome [because]…required information can be gathered throughout the year as part of managing the information security program and satisfying the other requirements of the proposed amendments.") (quoting proposed NPRM).

[9] *Id*. at 314.4(e) (requiring the hiring of qualified and sufficient personnel, continuous training for key personnel, and verification of training).

[10] *Id*. at 314.4(a)(1) (prohibiting companies from designating more than one employee to coordinate information security programs and instead requiring the designation of "a single qualified individual" (CISO)); *Id.* at 314.4(a)(2) (requiring oversight of CISO by appropriate senior member of personnel); *Id*. at 314.4(h) (requiring a written incident response plan).