Joint Statement of Commissioners Noah Joshua Phillips and Christine S. Wilson

In the Matter of the Final Rule amending the Gramm-Leach-Bliley Act's Safeguards Rule
Commission File No. P145407
October 27, 2021

In 1999, Congress passed the Gramm-Leach-Bliley Act, which charged the Federal Trade Commission (the "Commission") with promulgating and enforcing a regulation to ensure that financial firms take care to safeguard the information they collect from consumers.[1] The Safeguards Rule[2] has established more data security obligations for consumer financial data than for data collected by non-financial firms, a gap that underlies our view—shared by our colleagues—that congressional data security legislation is warranted.

One hallmark of the Safeguards Rule is its recognition that, in a world of continuously evolving threats and standards, a one-size-fits-all approach to data security may not work. Under Democratic and Republic leadership, the Commission has repeatedly emphasized this principle.[3] We have traditionally eschewed an overly prescriptive approach, both to data security in general and to the Safeguards Rule itself.[4] The FTC has never demanded "perfect" security because the Commission has recognized that data security is neither cost- nor consequence-free, and often

[1] Pub. L. 106–102, 113 Stat. 1338 (1999). Notably, even as it transferred authority for other consumer financial regulation to the Consumer Financial Protection Bureau in the Dodd-Frank Act, Congress left this rulemaking authority with the Commission, a vote of confidence in our approach. 15 U.S.C. § 6804(a)(1).

[2] 16 C.F.R Pt. 314.

[3] *See, e.g.,* Federal Trade Commission, Statement Marking the FTC's 50th Data Security Settlement, at 1 (Jan. 31, 2014), https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf ("FTC Data Security Statement") ("Through its settlements, testimony, and public statements, the Commission has made clear that it does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing risks; there is no one-size-fits-all data security program; and the mere fact that a breach occurred does not mean that a company has violated the law."); *see also* Prepared Statement of the Federal Trade Commission: Before the Committee on Homeland Security and Governmental Affairs Permanent Subcommittee on Investigations, 116 Cong. 3 (2019) (statement of Andrew Smith, Director, Bureau of Consumer Protection) ("[t]here is no one-size-fits-all data security program. . ."), https://www.ftc.gov/system/files/documents/public_statements/1466607/commission_testimony_re_data_security_senate_03072019.pdf. Federal Trade Commission, *Stick with Security: A Business Blog Series* (Oct. 2017), https://www.ftc.gov/news-events/blogs/business-blog/2017/10/stick-security-ftc-resources-your-business.

[4] FTC Notice of Proposed Rulemaking, 84 Fed. Reg. 13158 (Apr. 4, 2019), https://www.federalregister.gov/documents/2019/04/04/2019-04981/standards-for-safeguarding-customer-information ("The Commission continues to believe that a flexible, non-prescriptive Rule enables covered organizations to use it to respond to the changing landscape of security threats, to allow for innovation in security practices, and to accommodate technological changes and advances.").

requires tradeoffs.[5] At the same time, during our tenure, the Commission has continued to enforce data security standards vigorously, including those embodied in the Safeguards Rule.[6]

In March 2019, the Commission approved a Notice of Proposed Rulemaking ("NPRM") proposing additional requirements to the Safeguards Rule. While we recognize the value in regularly reviewing our rules and updating them as needed, we dissented then because the proposal lacked data demonstrating the need for and efficacy of the proposed amendments.[7]

We appreciate Staff's diligent work on this rule and many of the modifications made to the original proposal. The Federal Register Notice does a commendable job of presenting the full panoply of comments that the Commission received. The FTC is at its best when it seeks input from experts, industry, and consumer groups; this rulemaking process reflects a commitment to that approach. But the comment period did not produce data demonstrating that the previous iteration of the rule was inadequate, or that the costs and consequences of the new prescriptive obligations will translate into actual consumer safeguards. That was our concern, and the comments did not allay it.

In fact, as several commenters observed, the new prescriptive requirements could weaken data security by diverting finite resources towards a check-the-box compliance exercise and away from risk management tailored to address the unique security needs of individual financial institutions. It is ironic that the revisions mandate a risk assessment and then order firms to prioritize specified precautions ahead of the risks and needs counseled by that assessment. The revisions also impose intrusive corporate governance obligations wholly unsupported by record evidence of prevalent failures at the senior managerial level.

For these reasons, which we explain more fully below, we dissent.

---

[5] Under the FTC's unfairness authority, the Commission brings cases when companies under its jurisdiction fail to employ "reasonable" security. FTC Data Security Statement, *supra* note 3 ("The touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities.").

[6] *See, e.g., In the matter of Ascension Data & Analytics, LLC*, FTC File No. 1923126 (2020), https://www.ftc.gov/enforcement/cases-proceedings/192-3126/ascension-data-analytics-llc-matter; *U.S. v. Mortgage Solutions FCS, Inc.*, Civ. Action No. 4:20-cv-110 (N.D. Cal 2020), https://www.ftc.gov/enforcement/cases-proceedings/182-3199/mortgage-solutions-fcs-inc; *FTC v. Equifax, Inc.*, Civ. Action No. 1:19-cv-03297-TWT (N.D. Ga. 2019), https://www.ftc.gov/enforcement/cases-proceedings/172-3203/equifax-inc.

[7] Dissenting Statement of Commissioner Noah Joshua Phillips and Commissioner Christine S. Wilson, Review of Safeguards Rule (Mar. 5, 2019), https://www.ftc.gov/system/files/documents/public_statements/1466705/reg_review_of_safeguards_rule_cmr_phillips_wilson_dissent.pdf; *See, e,g*,, Noah Joshua Phillips (@FTCPhillips), Twitter (Mar. 5, 2019, 3:08 p.m.), https://twitter.com/FTCPhillips/status/1103024596247289867 ("A reexamination of the Rule may indeed be appropriate and necessary; but, before we borrow from other existing schemes, we must first understand whether the existing Rule is inadequate for its purpose and whether the data supports the efficacy of the alternatives."); Christine S. Wilson, Remarks at NAD 2020, One Step Forward, Two Steps Back: Sound Policy on Consumer Protection Fundamentals 7-8 (Oct. 5, 2020), https://www.ftc.gov/system/files/documents/public_statements/1581434/wilson_remarks_at_nad_100520.pdf.

The record fails to provide a basis for the new requirements

We expressed concern in March 2019 that some of the proposals in the NPRM tracked issues that arose in cases involving firms not covered by the Safeguards Rule. That is, those failures occurred at companies to which the Safeguards Rule did not apply. And heightened obligations imposed in a settlement context, when a company has engaged in risky and allegedly illegal behavior, may not be appropriate for all market participants. We did not see evidence that covered firms had a systematic problem—*i.e.,* that the Rule was not working.[8] The Commission can—and does— promote best practices and reasonable care requirements through speeches, guidance, reports, and the like, to help financial firms evaluate whether they are taking proper precautions.[9] But new rules that set concrete standards for all companies, regardless of risk, require more justification. Such rules make companies liable for penalties, and could focus efforts on compliance to address penalty deterrence rather than risk.

Dozens of commenters have shared their views on the Safeguards proposal, and FTC Staff held a workshop to evaluate the need to change the Rule. While there is no shortage of *opinions* as to the need and benefits of the proposed changes (nor is there a shortage of opinions critiquing the new requirements), this process failed to provide evidence of market failure or other systemic problems[10] necessitating the proposed changes for firms already governed by the requirements of the Rule. In fact, one commenter that generally supported the rule changes noted that it was not

---

[8] Commenters on the proposed rules reflected these same concerns. *See, e.g,* CTIA (comment 34, NPRM) at 4, https://www.regulations.gov/comment/FTC/2019-0019-0034 (observing that most examples cited in the NPRM are from non-financial firms and arguing that the FTC's action in Equifax demonstrated that the agency is able to use to the current framework effectively); Global Privacy Alliance (comment 38, NPRM) at 4, https://www.regulations.gov/comment/FTC/2019-0019-0038 (the changes to the rules started not from FTC experience but rather from state laws); Electronic Transactions Association (comment 27, NPRM), https://www.regulations.gov/comment/FTC/2019-0019-0027 (the current rule is effective and there are no harms that warrant these changes); National Automobile Dealers Association (comment 46, NPRM) at 6, https://www.regulations.gov/comment/FTC/2019-0019-0046 ("[N]ew requirements for *all* financial institutions should not be based on unrelated enforcement actions that may not be generally applicable to all financial institutions subject to the Rule.").

[9] Federal Trade Commission, *Data Security*, https://www.ftc.gov/datasecurity.

[10] One study cited by commenters pointed toward widespread problems among fintech firms "including misuse of cryptography, use of weak cryptography, and excessive permission requirements." The Clearing House Association LLC (comment 49, NPRM) at 7-9, https://www.regulations.gov/comment/FTC/2019-0019-0049 (citing a 2018 study by the Center for Financial Inclusion, https://content.centerforfinancialinclusion.org/wp-content/uploads/sites/2/2018/09/CFI43-CFI_Online_Security-Final-2018.09.12.pdf). This study included firms from around the world and did not indicate that this limited set of issues arose in U.S. firms covered by the Safeguards Rule. *See also* National Automobile Dealers Association (comment 46, NPRM) at 46, https://www.regulations.gov/comment/FTC/2019-0019-0046 ("These requirements have largely not been proven to be necessary or effective."). Participants at the FTC's July 2020 Workshop generally agreed that companies could invest more in security, but the fact of under-investment does not mean that these changes to the Safeguards Rule constitute the best course of action. FTC, Information Security and Financial Institutions: An FTC Workshop to Examine Safeguards Rule Tr. at 23-70 (July 13, 2020), https://www.ftc.gov/system/files/documents/public_events/1567141/transcript-glb-safeguards-workshop-full.pdf ("Safeguards Workshop").

clear that the new rules would have prevented the alleged lapses that led to the Equifax breach, the largest Safeguards case on record.[11]

That these proposals may constitute best practices appropriate to certain firms or situations does not justify imposing them on every firm and in every situation.[12] The FTC historically has been appropriately cautious in mandating specific security practices, and we see no sound basis in the rulemaking record to change that approach.[13]

The revised Safeguards Rule is premature

In our 2019 statement, we expressed concern that the proposals in the NPRM were premature. They are based in large part on the New York Department of Financial Service data security rules,[14] adopted in 2016. At the same time, Congress and the Executive Branch were evaluating new privacy and data security legislation that may overlap with the proposed amendments.[15]

---

[11] Consumer Reports (comment 52, NPRM), https://www.regulations.gov/comment/FTC/2019-0019-0052 at 2. Not all the commenters agreed with this perspective, and some felt that these rules would have prevented the Equifax breach. *See* National Consumer Law Center and others (comment 58, NPRM), https://www.regulations.gov/comment/FTC/2019-0019-0058. Chair Khan and Commissioner Slaughter focus on the Equifax breach to justify the adoption of prescriptive and complex data security measures, measures that match the sophistication and complexity of the consumer financial data managed by one of the largest credit bureaus. But even assuming the new rules would have prevented it, one (albeit) high-profile breach, without more, should not be extrapolated to an entire industry with diverse business models housing varied consumer financial data. Reasonable safeguards for a company like Equifax, based on its size and complexity, the nature and scope of its activities, and the sensitivity of the information involved, would likely outpace procedures that would be appropriate or reasonable for a sole proprietorship or small business.

[12] While the Final Rule is based on proposals from New York State Department of Financial Services ("NYDFS"), the FTC imposes its requirements much more broadly than the NYDFS Cybersecurity Requirements for Financial Services Companies, 23 NYCRR Pt. 500. The NYDFS requirements exempt a much larger cross-section of organizations from the most onerous, prescriptive, and expensive provisions in their rule. 23 NYCRR §500.19. Nor do the exceptions in the Final Rule, while helpful, suffice.

[13] Unfortunately, this is not the first time this Commission has emphasized what we *can* do over what we *should* do. *See, e.g.,* Joint Statement of Commissioners Noah Joshua Phillips and Christine S. Wilson, *In the matter of Resident Home LLC*, Commission File No. 2023179 (Oct. 7, 2021), https://www.ftc.gov/system/files/documents/public_statements/1597270/resident_home_dissenting_statement_wilson_and_phillips_final_0.pdf; Joint Statement of Commissioners Noah Joshua Phillips and Christine S. Wilson, *U.S. v. iSpring Water Systems, LLC*, Commission File No. C4611 (Apr. 12, 2019), https://www.ftc.gov/system/files/documents/public_statements/1513499/ispring_water_systems_llc_c4611_modified_joint_statement_of_commissioners_phillips_and_wilson_4-12.pdf.

[14] Cybersecurity Requirements for Financial Services Companies, 23 NYCRR Pt. 500 (2016).

[15] *See* Consumer Data Industry Association (comment 36, NPRM) at 2, https://www.regulations.gov/document?D=FTC-2019-0019-0036 (noting that the NY rule is too recent and Congress is debating new legislation that should be left to Congress to resolve); National Automobile Dealers Association (comment 46, NPRM) at 46, https://www.regulations.gov/comment/FTC-2019-0019-0046 (The new rules "are premature as they are based on untested and new standards in a rapidly changing environment, and in a context where federal debate is ongoing."); New York Insurance Association (comment 31, NPRM), https://www.regulations.gov/comment/FTC-2019-0019-0031 (it is premature to adopt these rules without the benefit of the state's experience).

Since our original statement, we have been provided with no additional information on the impact and efficacy of the NYDFS rules.[16] Without this critical input, we do not believe adopting wholesale the NYDFS approach is the prudent course.[17] We would have been better served by monitoring the efficacy, costs and unintended consequences of the NYDFS rules during this ramp-up period. Imposing similar rules on far more firms across a broader array of industries makes even less sense.

Congress, with the encouragement of the Commission, has continued to consider legislative initiatives in this area. Throughout 2019, 2020 and 2021, we saw the release of several draft bills addressing data security, as well as privacy.[18] And other developments, such as data security requirements of the General Data Protection Regulation[19] and new cybersecurity incidents[20] ensure that these issues will continue to draw congressional attention. The decisions about tradeoffs in this space are complex and significant for consumers, business, and government; intrusive mandates are best left to the people's representatives rather than to the vagaries of the administrative rulemaking process.[21]

---

[16] We appreciate the time and resources the NYDFS invested in commenting on our proposed rule. Though the NYDFS does say that its rules have "enhanced cybersecurity protection across the financial industry and fostered an environment in which the threat of a cyber attack is taken seriously at all levels of New York's financial services firms," it offers no supporting data. New York State Department of Financial Services (comment 40, NPRM), https://www.regulations.gov/comment/FTC-2019-0019-0040.

[17] As several commenters pointed out, the NYDFS rules are more nuanced that the amendments introduced today. For instance, under the NYDFS regulations, certain additional requirements only apply to a category of sensitive data, a limitation not carried through to the Safeguards Rule. *See, e.g.,* U.S. Chamber of Commerce (comment 33, NPRM), https://www.regulations.gov/comment/FTC-2019-0019-0033; CTIA (comment 34, NPRM), https://www.regulations.gov/comment/FTC/2019-0019-0034; Electronic Transactions Association (comment 27, NPRM), https://www.regulations.gov/comment/FTC/2019-0019-0027.

These distinctions only raise more questions and concerns about basing our regulations on the New York rules.

[18] *See, e.g.,* Fourth Amendment is Not for Sale Act, S. 1265, 117th Cong. (2021); Data Care Act of 2021, S. 919, 117th Cong. (2021); Data Protection Act of 2021, S. 2134, 117th Cong. (2021); SAFE DATA Act, S. 2499, 117th Cong. (2021); Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019). *See also*, California Privacy Rights Act of 2020, Cal. Civ. Code § 1798.100 *et seq.*; Virginia Consumer Data Protection Act, Va. Code § 59.1-575 *et seq.*; and Colorado Privacy Act, 2021 Colo. ALS 483, 2021 Colo. Ch. 483, 2021 Colo. SB. 190.

[19] Council Directive 2016/679, art. 32 2016 O.J. (L119).

[20] *See, e.g.,* Joseph Menn and Christopher Bing, *Hackers of SolarWinds stole data on U.S. sanctions policy, intelligence probes*, REUTERS (Oct. 8, 2021), https://www.reuters.com/world/us/hackers-solarwinds-breach-stole-data-us-sanctions-policy-intelligence-probes-2021-10-07/; Stephanie Kelly and Jessica Resnick-ault, *One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators*, REUTERS (June 8, 2021), https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08; Carly Page, *The Accellion data breach continues to get messier*, TECHCRUNCH (July 8, 2021), https://techcrunch.com/2021/07/08/the-accellion-data-breach-continues-to-get-messier/; Peter Valdes-Dapena, *Volkswagen hack: 3 million customers have had their information stolen,* CNN (June 11, 2021), https://www.cnn.com/2021/06/11/cars/vw-audi-hack-customer-information/index.html.

[21] Sen. Roger Wicker, Rep. Cathy McMorris Rodgers, & Noah Phillips, *FTC must leave privacy legislating to Congress*, WASH. EXAMINER (Sept. 29, 2021), https://www.washingtonexaminer.com/opinion/op-eds/ftc-must-leave-privacy-legislating-to-congress. Substance aside, businesses and consumers need confidence to plan around new rules. As the recent—and perhaps future—debate about net neutrality rules has demonstrated, agency rules are subject to disruptive swings that undermine such confidence.

The revised rules inhibit flexibility and impose substantial costs

The Safeguards Rule originally drafted and evaluated by the Commission embraced a flexible approach, emphasizing protections targeted to a company's size and risk profile.[22] As we wrote in 2019, these new rules move us away from that approach; that loss of flexibility will impose costs without necessarily improving safeguards for consumer data, which should be the point of this exercise.

Commenters and the Commission itself have noted that there are financial impacts to these new requirements.[23] The Small Business Administration's Office of Advocacy stated its belief that the Commission itself does not appear to understand fully the economic impact of the proposed changes to the Safeguards Rule.[24]

The burden of these new rules may also reduce competition and innovation, as smaller firms less able to absorb the financial costs cede ground to larger firms better equipped to handle new regulatory mandates.[25]

---

[22] The Commission itself acknowledges the importance of flexibility in issuing the Final Rule. *See, e.g.,* Final Rule at 27 ("The Commission, however, believes that the elements provide sufficient flexibility for financial institutions to adopt information security programs suited to the size, nature, and complexity of their organization and information systems.")

[23] *See* Final Rule; American Council on Education (comment 24, NPRM) at 13-14, https://www.regulations.gov/comment/FTC-2019-0019-0024; Wisconsin Bankers Association (comment 37, NPRM) at 1-2, https://www.regulations.gov/comment/FTC-2019-0019-0037; American Financial Services Association (comment 41, NPRM) at 4, https://www.regulations.gov/comment/FTC-2019-0019-0041; National Association of Dealer Counsel (comment 44, NPRM) at 1, https://www.regulations.gov/comment/FTC-2019-0019-0044; National Automobile Dealers Association (comment 46, NPRM) at 11, https://www.regulations.gov/comment/FTC-2019-0019-0046; National Independent Automobile Dealers Association, (comment 48, NPRM) at 3, https://www.regulations.gov/comment/FTC-2019-0019-0048; Gusto and others (comment 11, Workshop) at 2-4, https://www.regulations.gov/comment/FTC-2019-0019-0011; National Pawnbrokers Association (comment 3, NPRM) at 2, https://www.regulations.gov/comment/FTC-2019-0019-0032; *See also* Remarks of James Crifasi, Safeguards Workshop, *supra* note 10, Tr. at 72- 74, https://www.ftc.gov/system/files/documents/public_events/1567141/transcript-glb-safeguards-workshop-full.pdf (study showing that compliance costs are unaffordable for small businesses).

[24] Small Business Administration Office of Advocacy (comment 28, NPRM) at 3-4, https://www.regulations.gov/comment/FTC-2019-0019-0028 ("An agency cannot consider alternatives that minimize any significant economic impact if the agency does not know what the economic impact of the proposed action is.").

[25] *See* CTIA (comment 34, NPRM), https://www.regulations.gov/comment/FTC-2019-0019-0034 (noting the need for more study on the costs to competition); U.S. Chamber of Commerce (comment 33, NPRM) at 4, https://www.regulations.gov/comment/FTC-2019-0019-0033 ("Some private organizations can absorb the added costs, while others cannot."). *See also* Christine S. Wilson, Remarks at the Future of Privacy Forum, A Defining Moment for Privacy: The Time is Ripe for Federal Privacy Legislation 13 (Feb. 6, 2020), https://www.ftc.gov/system/files/documents/public_statements/1566337/commissioner_wilson_privacy_forum_speech_02-06-2020.pdf ("Importantly, the legislative framework should also consider competition. Regulations, by their nature, will impact markets and competition. GDPR may have lessons to teach us in this regard. Research indicates that GDPR may have decreased venture capital investment and entrenched dominant players in the digital advertising market."); Noah Joshua Phillips, Prepared Remarks at Internet Governance Forum USA, Keep It: Maintaining Competition in the Privacy Debate (July 27, 2018), https://www.ftc.gov/system/files/documents/public_statements/1395934/phillips_-_internet_governance_forum_7-27-18.pdf (discussing the competition impacts of new privacy rules).

Security itself may also suffer. A series of specific rules can incentivize companies to move from a thoughtful assessment of risk and precautions to a check-the-box exercise to ensure that they are complying with regulatory mandates—in other words, from a focus on real security to an emphasis on rule compliance.[26] One commenter cited data demonstrating that when security personnel are busy with compliance and regulatory response, they have less time to focus on a firm's actual security needs.[27] Further, without the flexibility to prioritize, finite resources may be diverted to areas of lower risk but higher regulatory scrutiny; [28] commenters noted the irony of mandating a risk assessment and then ordering firms to prioritize specified precautions ahead of the risks and needs counseled by that assessment.[29] And potentially innovative security

---

[26] *See* U.S. Chamber of Commerce (comment 33, NPRM), https://www.regulations.gov/comment/FTC-2019-0019-0033; Consumer Data Industry Association (comment 36, NPRM), https://www.regulations.gov/comment/FTC-2019-0019-0036; Global Privacy Alliance (comment 38, NPRM), https://www.regulations.gov/comment/FTC/2019-0019-0038. While some parts of the rule, such as encryption requirements, allow security officials to make a written determination that a different precaution is appropriate, it seems unlikely that any individual security official will risk liability to make such a determination and the specific requirements here will likely become the default rule. American Council on Education (comment 24, NPRM) at 12, https://www.regulations.gov/comment/FTC-2019-0019-0024("In the absence of a clear delineation by the Commission of what alternatives an institutional information security executive might approve that the Commission considers reasonably equivalent, and assurance that they are reasonably applicable in our contexts, that pressure release valve in the requirement seems unlikely to release much pressure."); Software Information & Industry Association (comment 29, NPRM) at 3, https://www.regulations.gov/comment/FTC-2019-0019-0056 ("The mere threat of a *per se* law violation will chill these approvals except in the most ironclad circumstances, thereby potentially thwarting industry-wide adoption of new and better security standards."); New York Insurance Association (comment 31, NPRM), https://www.regulations.gov/comment/FTC-2019-0019-0031 ("This runs the risk that companies might feel compelled to encrypt all consumer data regardless of whether the CISO's compensating controls would be second guessed in the event a company were to lose unencrypted customer information."); Mortgage Bankers Association (comment 26, NPRM) at 4, https://www.regulations.gov/comment/FTC-2019-0019-0026 (noting the obligation to prepare an incident response plan had "the potential to cripple small businesses under the pressure of repeatedly checking the boxes for potential harmless events.").

[27] Bank Policy Institute (comment 39, NPRM) at 6, https://www.regulations.gov/comment/FTC-2019-0019-0039 ("When the sector surveyed its information security teams in late 2016, CISOs reported that approximately 40% of their cyber team's time was spent on compliance related matters, not on cybersecurity. Due to one framework issuance, in particular, the reconciliation process delayed one firm's implementation of a security event monitoring tool intended to better detect and respond to cyber-attacks by 3-6 months. With respect to another issuance, another firm stated that 91 internal meetings were held to determine how that issuance aligned with its program and in gathering data for eventual regulatory requests.").

[28] *See* U.S. Chamber of Commerce (comment 33, NPRM) at 4, https://www.regulations.gov/comment/FTC-2019-0019-0033 ("the proposed requirements would increasingly divert company resources toward compliance and away from risk management activities that are tailored to businesses' unique security needs."); Software Information & Industry Association (comment 29, NPRM) at 3, https://www.regulations.gov/comment/FTC-2019-0019-0056 ("The effect of a prescriptive approach in this enforcement structure is to place companies in the position of forced compliance with potentially unnecessary or inapplicable requirements without the appropriate process for these covered entities to explain to a supervisory authority why it is unnecessary."); American Financial Services Association (comment 41, NPRM), https://www.regulations.gov/comment/FTC-2019-0019-0041. In some cases, asking too much of small businesses for whom all this is a substantial undertaking may lead them to fail at even the basic protections. Safeguards Workshop, *supra* note 10, Tr. at 118-19 (July 13, 2020), https://www.ftc.gov/system/files/documents/public_events/1567141/transcript-glb-safeguards-workshop-full.pdf.

[29] *See* Bank Policy Institute (comment 39, NPRM), https://www.regulations.gov/comment/FTC-2019-0019-0039; Money Services Round Table (comment 53, NPRM), https://www.regulations.gov/comment/FTC-2019-0019-0053.

practices that address changing threats and needs may be discouraged.[30] As one commenter noted, "[e]ven today's best practices will be overtaken by future changes in both technology and the capabilities of threat actors,"[31] and these proscriptive rules lose the "self-modernizing" nature of flexible requirements,[32] locking in place the primacy of current practices.[33]

The reduction in flexibility and imposition of these costs must be justified by a significant reduction in risk or some other substantial consumer benefit. But the record provides scant support for these tradeoffs. Or as one commenter put it:

> [A]s with many of these requirements, we do not take issue with the notion that there is merit to this step [requiring monitoring], and that many financial institutions will implement some version of this control. However, by making this an explicit, stand-alone requirement, the Commission is enshrining costs and efforts that will be extensive and will likely not be needed in all circumstances."[34]

The rules involve the FTC in the internal governance decisions of covered firms

The specifics of the proposals also raise issues, as we expressed in 2019, with regard to mandating the appropriate level of board engagement,[35] hiring and training requirements,[36] and program accountability structures.[37] We wrote then, and remain concerned now, that the

---

[30] *See* Consumer Data Industry Association (comment 36, NPRM) at 7-8, https://www.regulations.gov/comment/FTC-2019-0019-0036 (minimization requirement can impact innovative uses more broadly).

[31] *See* Cisco Systems Inc. (comment 51, NPRM) at 3, https://www.regulations.gov/comment/FTC-2019-0019-0051 (noting also in the context of multi-factor authentication that there will come a time when it is no longer the "appropriate baseline" and "covered entities could find themselves in full compliance with the rule as long as they use access control technology no less protective than MFA as defined in the Proposed Amendments.").

[32] National Automobile Dealers Association (comment 46, NPRM), https://www.regulations.gov/comment/FTC-2019-0019-0046.

[33] *See* CTIA (comment 34, NPRM) at 3-5, https://www.regulations.gov/comment/FTC-2019-0019-0034 (flexibility in the rule allowed it to keep up with evolving threats, whereas new rule could limit innovation); HITRUST Alliance (comment 18, NPRM), https://www.regulations.gov/comment/FTC-2019-0019-0018 (expressing concern about creating outdated requirements); The American Financial Services Association (comment 41, NPRM), https://www.regulations.gov/comment/FTC-2019-0019-0041.

[34] National Automobile Dealers Association (comment 46, NPRM) https://www.regulations.gov/comment/FTC-2019-0019-0046 (arguing that the Commission needs additional study into the costs and benefits); *See* also Consumer Data Industry Association (comment 36, NPRM), https://www.regulations.gov/comment/FTC-2019-0019-0036 (benefits of new rule not justified by tradeoffs).

[35] American Council on Education (comment 24, NPRM) at 16, https://www.regulations.gov/comment/FTC-2019-0019-0024; National Automobile Dealers Association (comment 46, NPRM) at 41, https://www.regulations.gov/comment/FTC-2019-0019-0046.

[36] U.S. Chamber of Commerce (comment 33, NPRM) at 12, https://www.regulations.gov/comment/FTC-2019-0019-0033; National Automobile Dealers Association (comment 46, NPRM) at 34-36, https://www.regulations.gov/comment/FTC-2019-0019-0046.

[37] *See* Final Rule. *See* also American Council on Education (comment 24, NPRM) at 14, https://www.regulations.gov/comment/FTC-2019-0019-0024 (critiquing the intrusion on personnel practices).

Commission is substituting its own judgement about governance decisions for those of private companies covered by this Rule.

In certain extraordinary cases involving clear evidence of management failure, we have imposed prescriptive governance obligations on respondents.[38] Those rare and egregious instances cannot justify a similar approach in a broad rulemaking absent a real record of widespread corporate mismanagement or failure at the senior management level.

The Commission has elected to proceed with most of these governance requirements, forcing the hand of management and shifting their priorities to avoid the risk of regulatory action,[39] without clear evidence of their need or efficacy.

Conclusion

Regularly reviewing our rules to ensure that they address the current environment is an important part of the FTC's regular process. But rules have far-reaching and frequently unintended impacts in the real world; when imposing additional legal obligations in the rulemaking context, we must do so with great care. The amended Safeguards Rule replaces a rule that has worked well for 20 years, a rule that took a principle-based approach in order to provide financial institutions flexibility to determine the appropriate and realistic security safeguards for their organizations. The record before us at best fails to convince that the changes are necessary and at worst raises concern about the substantial costs and risks in imposing these amendments. Accordingly, we dissent.

[38] *U.S. v. Facebook, Inc.*, Civ. Action No. 19-cv-2184 (D.D.C. July 24, 2019), https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc.

[39] These governance rules may not even promote security. *See* Consumer Data Industry Association (comment 36, NPRM), https://www.regulations.gov/comment/FTC-2019-0019-0036 (arguing that the annual reporting will become a checkbox exercise).