Statement of Chair Lina M. Khan  
Joined by Commissioner Rebecca Kelly Slaughter  
Regarding Regulatory Review of the Safeguards Rule  
Commission File No. P145407  
October 27, 2021

Today the FTC is significantly strengthening the Safeguards Rule,1 first promulgated by the FTC twenty years ago pursuant to a Congressional directive to protect personal information that is stored by financial institutions. This revamping—the first time in the Rule’s history—is sorely needed. In the twenty years since the Rule was first issued, the complexity of information security has increased drastically, the use of computer networks in every aspect of life has expanded exponentially, and, most notably, an unending chain of damaging data breaches caused by inadequate security have cost Americans heavily.2 The amendments adopted today require financial institutions to develop information security programs that can meet the challenges of today’s security environment.

For Americans, the harms stemming from the types of security vulnerabilities that this Rule addresses are all too real. Victims of breaches have their most sensitive information exposed, making them more vulnerable to identity theft, phishing attacks, and other forms of fraud.3 In 2018, almost 10 percent of Americans suffered some form of identity theft, costing many of them hundreds of dollars and dozens of hours of time, an experience that many describe as distressing.4 For some, the cost is much higher, with victims losing tens of thousands of dollars.5

---

3 2013 IDENTITY FRAUD REPORT: DATA BREACHES BECOMING A TREASURE TROVE FOR FRAUDSTERS, JAVELIN STRATEGY, at 1 (Feb. 2013) (reporting that 1 in 4 recipients of a data breach notification become victims of identity theft); Michelle Singletary, Your online profile may help identity thieves, WaPo, (Feb. 28, 2012), https://www.washingtonpost.com/business/economy/michelle-singletary-your-online-profile-may-help-identity-thieves/2012/02/28/qI0AXFyggR_story.html (reporting that recipients of data breach letters are 9.5% more likely to suffer identity theft).
5 See 2021 CONSUMER AFTERMATH REPORT, IDENTITY THEFT RESOURCE CENTER (2021), at 6 (finding that in a study of 427 identity crime victims, 21% of them suffered losses of over $20,000).
The Rule amendments the FTC is issuing today are strongly supported by the evidence in the record. The evidence gathered from information security experts, industry associations, and consumer groups—those with hands-on experience in the area and knowledge of the field—decisively show that the amendments are necessary. Of course, all of this information supplements the experience that Commission staff has obtained over twenty years of enforcing the Rule, and gained through investigations of companies’ data security practices under the FTC’s deception and unfairness authority.

The dissent’s conclusion that these amendments are unnecessary is belied by both the reality of rampant data security breaches as well as the robust evidentiary record. The recent history of major data breaches affecting millions of consumers shows that more needs to be done to protect consumers’ sensitive information. Despite the increasing sophistication of cyberattacks, many businesses continue to offer inadequate security.

---


Equifax breach, which the FTC alleged was caused by inadequate data security that could have been easily corrected by the company, is a glaring example of how a financial institution’s lax security practices can have devastating consequences for Americans.8 The dissent’s suggestion that our current framework is sufficient falls flat in the face of such a stark example of the harm that can arise from avoidable lax security practices by covered financial institutions. Moreover, the dissent’s complaint that the rule is also informed by evidence arising from breaches and practices occurring in other types of industries misses the mark. Not only is there substantial evidence in the rulemaking record clearly illustrating security lapses of financial institutions that are covered by the Rule,9 but the implication that we shouldn’t use our broader knowledge of common security pitfalls is unwise.

The record evidence also shows that the amendment’s requirements track bedrock principles of data security and represent proven elements of effective data security programs that reduce the risk of breaches.10 The amended Rule requires that financial institutions’ information

---


9 See infra note 7.

10 See, e.g., for Single Qualified Individual Requirement: National Consumer Law Center et al., supra note 7, at 3 (arguing that a clear line of reporting with a single responsible individual could have prevented the Equifax consumer data breach); Safeguards Workshop, at 182-84 (remarks of Adrienne Allen) (stating that without a single responsible individual, information security staff “can fall into traps of each relying on someone else to make a hard call. . . . In a program without a single coordinator] issues can sometimes fall through the cracks.”). Id. at 184-85 (remarks of Michele Norin) (“I think it’s extremely important to have a person in front of the information security program. I think that there are so many components to understand, to manage, to keep an eye on. I think it’s difficult to do that if it’s part of someone else’s job. And so I found that it’s extremely helpful to have a person in charge of that program just from a pure basic management perspective and understanding perspective.”); Risk Assessment Requirement: Id. at 25 (remarks of Chris Cronin) (stating that evaluating the likelihoods and impacts of potential security risks and evaluating existing controls is an important component of a risk assessment). Id. at 29-30 (remarks of Serge Jorgensen) (emphasizing the importance of risk assessments as tools for adjusting existing security measures to account for both current and future security threats); Encryption Requirement: Princeton University Center for Information Technology Policy, Comment Letter No. 54 on 2019 Safeguards and Privacy NPRM (FTC-2019-0019), at 3 (Aug. 2, 2019), https://www.regulations.gov/document/FTC-2019-0019-0054 (noting the effectiveness of encryption); Inpher, Inc., supra note 7, at 4; Safeguards Workshop, at 225 (remarks of Matthew Green) (noting website usage of encryption is above 80 percent; “Let’s Encrypt” provides free TLS certificates; and costs have gone down to the point that if a financial institution is not using TLS encryption for data in motion, it is making an unusual decision outside the norm). Id. at 106 (remarks of Rocio Baeza) (“[The encryption of data in transit has been standard. There’s no pushback with that.”)); Multifactor Authentication Requirement: Princeton University Center for Information Technology Policy, supra note 10, at 6-7; Electronic Privacy Information Center, supra, note 7, at 8; National Consumer Law Center et al., supra note 7, at 2; Safeguards Workshop, at 102 (remarks of Brian McManamon) (stating that his company TECH LOCK supports requiring multi-factor authentication for...
security plans address such core concepts as controlling who is accessing their system, understanding their system, monitoring what users do in their system, and protecting the information contained in their system. More particularly, it also requires encryption of customer information and the use of multifactor authentication. Adopting these practices will reduce the chances of a breach occurring.

In fact, it is likely that the massive breach at Equifax could have been prevented or mitigated by adopting practices required by these amendments. For example, the Commission’s complaint alleged that the vulnerability that led to the breach was not detected for four months because Equifax’s automated vulnerability scanner was not configured to scan all of the networks in the system, something that could have been prevented if Equifax had performed an adequate inventory of its system as required by section 314.4(c)(2) of the amended Rule. Equifax allegedly did not encrypt the data of 145 million consumers as required by section 314.4(c)(3) of the amended Rule; such encryption might have prevented the intruders from misusing individuals’ sensitive information, even if they were able to obtain it. In addition, the complaint charged that Equifax did not adequately monitor activity on its network, which allowed intruders to access and use their network undetected for months; such monitoring will be

users connecting from internal networks. \textit{Id.} at 266 (remarks of Matthew Green) (explaining that passwords are not enough of an authentication feature but when MFA is used and deployed, the defenders can win against attackers). \textit{Id.} at 239 (describing how because smart phones have modern secure hardware processors, biometric sensors and readers built in, increasingly consumers can get the security they need through the devices they already have by storing cryptographic authentication keys on the devices and then using the phone to activate them). \textbf{Incident Response Plan:} Credit Union National Association, Comment Letter No. 30 on 2019 Safeguards and Privacy NPRM (FTC-2019-0019), at 2 (Aug. 1, 2019), https://www.regulations.gov/document/FTC-2019-0019-0030 (noting that that an incident response plan “helps ensure that an entity is prepared in case of an incident by planning how it will respond and what is required for the response.”). Consumer Reports, supra note 7, at 6 (observing that “a written incident response plan is an essential component of a good security system.”); HITRUST, Comment Letter No. 18 on 2019 Safeguards and Privacy NPRM (FTC-2019-0019), at 2 (July 1, 2019), https://www.regulations.gov/document/FTC-2019-0019-0018 (commenting that incident response plans can help organizations “to better allocate limited resources.”). Safeguards Workshop, at 52 (remarks of Serge Jorgenson) (observing that a prompt response to an incident can prevent a “threat actor running around in my environment for days, months, years, and able to access anything they want.”); \textbf{Board Reporting Requirement:} Workshop participants Adrienne Allen, Karthik Rangarajan, and Michele Norin each emphasized that such reporting can aid decision making. See Safeguards Workshop, at 201-09; see also Rocio Baeza, Comment Letter No. 12 on Workshop Comment Docket (FTC-2020-0038), at 3-8 (Aug. 12, 2020), https://www.regulations.gov/comment/FTC-2020-0038-0012 (supporting requirement and providing sample report form and compliance questionnaire); Juhee Kwon et al., \textit{The Association Between Top Management Involvement and Compensation and Information Security Breaches,} J. L. INFO. SYS., at 219-236 (2013) (“…the involvement of an IT executive decreases the probability of information security breach reports by about 35 percent…”); Julia L. Higgs et al., \textit{The Relationship Between Board-Level Technology Committees and Reported Security Breaches,} J. L. INFO. SYS., at 79-98 (2016) (“[A] technology committee becomes more established, its firm is not as likely to be breached. To obtain further evidence on the perceived value of a technology committee, this study uses a returns analysis and finds that the presence of a technology committee mitigates the negative abnormal stock returns arising from external breaches.”).

11 16 C.F.R. § 314.4(c)(1).
12 \textit{Id.} § 314.4(c)(2).
13 \textit{Id.} § 314.4(c)(8).
14 \textit{Id.} §§ 314.4(c)(3), (5).
16 \textit{Id.} ¶ 22.E.
required by section 314.4(c)(8).\textsuperscript{17} Finally, and perhaps most importantly, Equifax split authority over its information security program between two people, which caused failures of communications and oversight.\textsuperscript{18} Indeed, the U.S. House Committee on Oversight and Government identified Equifax’s organization as one of the major causes of the breach.\textsuperscript{19} Appointing a single Qualified Individual as the coordinator of Equifax’s information security system, as required by section 314.4(a) of the amended Rule, could have helped prevent or limit the scope of one of the largest breaches in American history. By implementing the measures required in the amended Rule, financial institutions will prevent or mitigate many future breaches, protecting consumers and their information.

There is also no support for the dissent’s notion that the amendments eliminate financial institutions’ flexibility in a way that will hurt smaller businesses. The amendments require that information security programs address certain aspects of security, but do not prescribe any particular method for doing so. Specifically, the amended Rule requires that the information security program address areas such as access control, change management, information disposal, and monitoring user activity, but it does not require that financial institutions take any particular action in those areas. In fact, the Rule recognizes the concerns of small businesses and adopts appropriate flexibilities. Section 314.6 of the revised Rule exempts financial institutions that maintain information concerning fewer than 5,000 consumers from certain requirements. In addition, financial institutions with smaller and simpler systems may determine that minimal procedures are required in those areas, and they retain flexibility under these amendments to follow that route. Moreover, the record contains significant evidence that there are free and low-cost solutions for smaller businesses with more modest data security needs.\textsuperscript{20}

\textsuperscript{17} Id. ¶ 22.F.
\textsuperscript{18} While the dissent questions the requirements in the Rule regarding elevating security issues to the top levels of the corporate structure, research supports these requirements. Boards are becoming increasingly involved in cybersecurity governance, as demonstrated by surveys of practitioners and the growth of literature aimed at educating board members on cybersecurity. Some studies suggest that Board attention to data security decisions can dramatically improve data safeguarding. For example, one study found a 35% decrease in the probability of information security breaches when companies include the Chief Information Security Officer (or equivalent) in the top management team and the CISO has access to the board. See Juhee Kwon et al., supra note 10. see also Safeguards Workshop, at 201-09.
\textsuperscript{20} See, e.g., Safeguards Workshop, at 267 (remarks of Wendy Nather) (“we have a lot more options, a lot more technologies today than we did before that are making both of these solutions, both encryption and MFA, easier to use, more flexible, in some cases cheaper, and we should be encouraging their adoption wherever possible.”). Id. at 265-66 (remarks of Matthew Green) (“I think that we’re in a great time when we’ve reached the point where we can actually mandate that encryption be used. . . . And we’ve reached the point where now it is something that’s come to be and we can actually build well.”). Id. at 229-30 (remarks of Randy Marchany) (noting that encryption is already built into the Microsoft Office environment and that a number of Microsoft products, such as Spreadsheets, Excel, Docs, and PowerPoint, support that encryption feature). Id. at 225. Id. at 106 (Remarks of Rocio Baeza) (“[T]he encryption of data in transit has been standard. There’s no pushback with that.”). Id. at 74 (remarks of James Crifasi) (stating that car dealerships can rely on existing staff for the role of Qualified Individual). Id. at 78-79 (remarks of Lee Waters) (stating that any dealership with any IT staff at all would have someone who could assume the role of “qualified individual,” perhaps requiring some additional research or outside help). Id. at 81-82 (remarks of Rocio Baeza) (stating that companies may use an existing employee for the role and “for any areas where there may be skill gaps, that can be supplemented with either certifications or some type of education.”). Id. at 89-90
We believe that these amendments represent a much-needed step forward in protecting Americans’ data security. Given growing recognition that the requirements captured in the Rule represent best practices, some financial institutions seem to have already taken appropriate steps to protect customers’ data and meet the requirements set out in the amended Rule. It is important, though, to require those that lag behind to strengthen their security and prevent future breaches before they occur, rather than in the wake of a devastating breach after the damage has already been done.