Key Financial Data Security Takeaways From FTC Workshop

By **Janis Kestenbaum, Amelia Gerlicher and Erin Earl** (July 28, 2020)

Janis Kestenbaum

Amelia Gerlicher

Erin Earl

On June 13, the Federal Trade Commission held a virtual workshop on proposed changes to the Gramm-Leach-Bliley Act safeguards rule.[1]

Unchanged since it was issued in 2002, the safeguards rule imposes data security requirements on nonbank financial institutions, such as many fintech companies, universities, auto dealers, and mortgage brokers or other nondepository lenders.

The FTC used the original rule as a blueprint for data security requirements and consent orders under Section 5 of the Federal Trade Commission Act, and the agency may take a similar approach with the modified rule.

In its current form, the rule takes a wholly process-based approach. The rule requires an organization to develop, implement and maintain a written comprehensive information security program containing administrative, technical and physical safeguards for customer information that are appropriate to the business's size and complexity, the nature and scope of its activities, and the sensitivity of its customer information.

Financial institutions must conduct risk assessments to identify reasonably foreseeable risks to customer information. They must then design, implement and monitor safeguards to address the identified risks to customer information.

In 2019, the FTC issued a notice of proposed rulemaking to update the safeguards rule and sought public comment.[2] The proposal, which is modeled on the New York State Department of Financial Services cybersecurity regulation, retains the requirement of a written comprehensive information security program.

But it would significantly expand many existing process-based requirements, such as by requiring written incident response plans, mandating written reports from the chief information security officer to the business's board of directors or equivalent governing body, and imposing more detailed requirements as to the content of the security program.

In addition, in a fundamental departure from the current rule, the proposal would mandate specific measures, such as encryption, multifactor authentication, annual penetration testing and biannual vulnerability assessments. Financial institutions that maintain the customer information of fewer than 5,000 consumers would be exempt from many of these requirements.

At the workshop, the FTC heard from representatives of the security industry, universities and fintech about the proposed changes. Their discussion touched on some of the key issues raised by the proposal. Below we address those points as well as some critical issues and perspectives that were not addressed but that should be considered by the FTC before issuing a final rule.

Multifactor Authentication and Encryption

The proposed rule would require multifactor authentication, which is defined as authentication through at least two of the following: (1) something known, like a password, (2) something possessed, like a token, and (3) something inherent, like biometric information, for any individual accessing customer information or internal networks that contain customer information unless the chief information security officer has approved in writing the use of reasonably equivalent or more secure access controls.

The proposed rule would similarly require encryption for "all customer information held or transmitted ... both in transit over external networks and at rest," except if the financial institution determines doing so would be infeasible and the information is secured with "effective alternative compensating controls reviewed and approved by" its chief information security officer.

As the costs of encryption have decreased, and as tools to implement multifactor authentication have become more available, use of these technologies has grown.[3] In addition, the FTC for some time has encouraged or required the use of encryption and, more recently, multifactor authentication in its business guidance and orders.[4] The FTC's proposal would make these measures mandatory for nonbank financial institutions in a wide range of circumstances.

However, as one panelist pointed out, there may be circumstances in which compliance may impose operational difficulties, such as customers including their own information in unencrypted communications with the enterprise, exchanging email attachments, or interacting with cloud vendors that do not provide clients with control over storage and access protocols.

The FTC has underscored the importance of flexibility in the rule. The proposed rule acknowledges that encryption may pose particular operational challenges in some circumstances and that financial institutions should be permitted to institute alternative controls in such situations, provided the institution's chief information security officer reviews and approves the alternative safeguards and, similarly, that a chief information security officer may approve reasonably equivalent access controls in lieu of multifactor authentication.

But the workshop discussion did not shed light on the situations in which the FTC would be likely to agree that encryption would be infeasible or what types of controls would be deemed acceptable in the place of encryption or multifactor authentication.

To the contrary, some panelists argued that neither intellectual property restrictions nor behavioral analysis were adequate substitutes for multifactor authentication. The notice of proposed rulemaking likewise does not offer insight into these questions. For the FTC to offer meaningful flexibility to financial institutions, the commission commentary accompanying the final rule or staff guidance issued simultaneously or shortly thereafter should do so.

Challenges for Small Businesses

The workshop made clear that the FTC and relevant stakeholders are concerned about the impact the proposed rule may have on small businesses. One panelist, James Crifasi of RedZone Technologies LLC, estimated the cost of compliance with the proposed rule to be

two to three times the cost of compliance with the current safeguards rule.

The FTC and stakeholders also discussed whether the proposed small business exemption used the best threshold. Under the proposal, financial institutions that maintain customer information concerning fewer than five thousand consumers would be exempt from many of the proposed rule's requirements.[5] The 5,000 cutoff appears to have its origins in the FTC's 2012 report on protecting consumer privacy in an era of rapid change.[6] However, the FTC has never implemented the standard in a rule, to our knowledge.

Although styled a small business exemption, it may actually be limited to microbusinesses. By comparison, the small business exemption of the California Consumer Privacy Act views 50,000 California consumers, households or devices as a relevant threshold. Bipartisan federal privacy legislation likewise would look to whether a business processed the personal information of fewer than 100,000 individuals or even one million individuals.[7]

If the FTC is genuinely interested in relieving small businesses from the more onerous and prescriptive components of the proposed regulation, it should consider increasing the 5,000 individual cap to something at least comparable to the bipartisan privacy law proposals.

Board of Directors' Involvement

The notice of proposed rulemaking would require a business's chief information security officer to report in writing, at least annually, to the board of directors, equivalent governing body or senior officer responsible for the information security program on the status of the information security program and compliance with the safeguards rule, and other matters related to the information security program.[8]

Panelists generally commended this requirement. Rocio Baeza of CyberSecurityBase noted that the reporting requirement may be beneficial in conveying potential risks to the board, but without the proper guardrails could become a burdensome administrative task that outweighs its benefit.

Some panelists, by contrast, urged greater board involvement. For example, one panelist, Kiersten Todt of the Cyber Readiness Institute, suggested that, depending on the business, more frequent reporting may be appropriate to facilitate an ongoing and evolving conversation between the chief information security officer and the board as potential cybersecurity threats arise.

Other panelists argued that the board, informed by the chief information security officer 's technical expertise, should be involved in any decision to use safeguards other than encryption or multifactor authentication.

Requiring even greater board involvement would contravene basic principles regarding the appropriate role of a board of directors, which are not typically involved in day-to-day business decisions.[9] Although the FTC has required greater board oversight of data security in recent consent orders,[10] case-specific obligations are fundamentally different than imposing requirements via a rule.

In addition, the proposed requirement to present an annual review to senior leadership is in line with the FTC's broader effort to require more board oversight on data security decisions, and any more granular board involvement on data security may be expensive and time-consuming without any demonstrable benefits to outweigh these costs.

Impact of the Proposed Rules on Data Breach Notification Laws

The commission has expressed concern that the proposed rule should not undermine state breach notice reporting requirements,[11] which require businesses to report certain breaches to state regulators and/or affected individuals. While not discussed at the workshop, the proposed rule risks undermining such laws.

A number of states deem businesses compliant with their breach notification statutes — and thus exempt from notice requirements — where the business has complied with federal requirements to develop breach response procedures.[12] Currently, banks and credit unions are subject to interagency guidelines promulgated by their primary federal regulators that require both incident response planning and individual and regulatory notification following a breach.

Thus, even when state laws exempt banks and credit unions, those entities remain under breach reporting requirements at the federal level. By contrast, nonbank financial institutions currently are not subject to federal breach reporting or incident response requirements, so they generally must comply with state-level notice requirements, as applicable.

The proposed rule may unwittingly upset this regime. In states with the type of exemption described above, businesses would likely be exempt from providing consumer notice if they comply with the revised safeguards rule's requirement for an incident response plan — the result the FTC has said it wants to avoid. Given the varied ways in which state notification laws treat financial institutions, the FTC may wish to reconsider the incident response plan requirement in this already heavily regulated space.

What to Watch For

The timeline for when the commission will finalize the rule is unclear. One panelist, Randy Marchany of Virginia Polytechnic Institute and State University, urged the commission to delay imposition of new requirements while businesses continue to deal with COVID-19.

However, the FTC often works most quickly when a presidential election is in the offing or has just occurred — whether or not the president is reelected — as the head of the agency and/or the head of the Bureau of Consumer Protection work to bring matters to completion during their tenure. It is therefore possible the FTC will move quickly to finalize the rule.

Janis Kestenbaum and Amelia M. Gerlicher are partners, and Erin K. Earl is counsel, at Perkins Coie LLP.

Natasha Amlani, an associate at the firm, contributed to this article.

[1] FTC, Information Security and Financial Institutions: FTC Workshop to Examine Safeguards Rule (July 13, 2020), https://www.ftc.gov/news-events/events-calendar/information-security-financial-institutions-ftc-workshop-examine.

[2] FTC, Standards for Safeguarding Customer Information, 84 Fed. Reg. 13158 (Apr. 4, 2019).

[3] See, e.g., LastPass, Global Password Security Report (2019); Ponemon Institute, 2016 Global Encryption Trends Study (2016).

[4] See, e.g., FTC, Bus. Ctr. Blog, Stick with Security: Require secure passwords and authentication (Aug. 11, 2017); FTC, Bus. Ctr. Blog, Stick with Security: Store sensitive personal information securely and protect it during transmission (Aug. 18, 2017); FTC, Privacy & Security Update: 2019 (Feb. 2020).

[5] Proposed Rule § 314.6.

[6] See FTC, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (2012), available at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[7] See, e.g., Consumer Online Privacy Rights Act, S.2968, 116th Cong. (2019) (introduced by Sen. Cantwell, D-WA); United States Data Privacy Act of 2019, 116th Cong. (2019) (Discussion Draft of Staff of Sen. Wicker, R-MS); United States Consumer Data Privacy Act of 2020, S.3456 (2020) (introduced by Sen. Moran, R-KS) (defining "small business" as one that processes personal information of fewer than 1,000,000 individuals or sensitive personal information of fewer than 100,000 individuals).

[8] Proposed Rule § 314.4(i).

[9] See, e.g., Business Roundtable, "Principles of Corporate Governance, Principles of Corporate Governance," Harv. L. Sch. Forum on Corp. Governance (Sept. 8, 2016), https://corpgov.law.harvard.edu/2016/09/08/principles-of-corporate-governance/.

[10] FTC, Bus. Ctr. Blog, New and Improved FTC Data Security Orders: Better Guidance for Companies, Better Protection for Consumers (Jan. 6, 2020).

[11] Standards for Safeguarding Customer Information, 84 Fed. Reg. at 13170 & n.123.

[12] See, e.g., Colo. Rev. Stat. § 6-1-716 ("An individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this section.").