August 2, 2019

Via https://www.regulations.gov/document?D=FTC-2019-0019-0011

David Lincicum
Allison M. Lefrak
Division of Privacy and Identity Protection
Bureau of Consumer Protection
Federal Trade Commission
Washington, D.C. 20580

Subject: Safeguards Rule, 16 CFR part 314, Project No. P145407

Dear Mr. Lincicum and Ms. Lefrak:

The U.S. Chamber of Commerce welcomes the opportunity to comment on the Federal Trade Commission's (FTC's or the Commission's) proposed amendments to the Standards for Safeguarding Customer Information, more commonly known as the Safeguards Rule. We appreciate the substantial work that you and your colleagues put into developing it, your engagement with our Cybersecurity Working Group, and the deadline extension.[1]

This letter has three parts: First, it calls attention to the constructive aspects of the proposed rulemaking. Second, it urges policymakers, including the FTC and Congress, to streamline the rapidly growing number of data security/cybersecurity regulations that confront businesses domestically and internationally. Third, it recommends changes to the Commission's proposed modifications to the Safeguards Rule (pages 5–14).

Summary

- The Federal Trade Commission's (FTC's or the Commission's) Safeguards Rule proposal features positive elements, including not to create any independent reporting or notification requirements for financial institutions and to exempt small businesses from certain mandates of the regulation.
- The Chamber is concerned that a number of the Commission's proposed modifications to the Safeguards Rule would conflict with our long-standing interest in fostering a dynamic approach to cybersecurity governance. We particularly urge the FTC and other policymaking bodies to collaborate with industry to *streamline* the myriad data security/cybersecurity regulations, not increase them.
- The Chamber is not yet convinced that expanding the Safeguards Rule is necessary to achieve the Commission's mission, or that it would strengthen U.S. data security and/or cyber goals. We urge the Commission to refrain from modifying it.

RECOGNIZING THE POSITIVE

The FTC's proposal features constructive elements that should be recognized. First, the Chamber commends the Commission's decision not to "create any independent reporting or notification requirements," which could conflict with mandates that financial institutions are already subject.[2] This decision is sound. We believe that consumers should be notified as soon as reasonably possible following the discovery of a reportable data breach. Rather than specifying a specific time frame, the Chamber recommends policies that permit maximum flexibility, especially given the difficulties and uncertainties of responding to a data breach.[3]

Further, businesses that suffer a cyber incident need to first secure a hacked information system before identifying and notifying affected people. In a nutshell, it takes time to discover a breach, secure the impacted networks, and identify impacted consumers. A rigid time frame is unworkable.

Second, the Chamber applauds the agency's determination to newly exempt small businesses, many of which may have relatively few customers, from certain requirements of the Safeguards Rule.[4] More than 96% of Chamber member companies have fewer than 100 employees. We agree with skeptics of the Safeguards Rule expansion, who caution that it would create challenges for small businesses.[5]

Third, the Chamber urges private organizations to commit to robust data security/cybersecurity practices and regular enhancements. We launched our cybersecurity roundtable series in 2014 to promote the Cybersecurity Framework. This national initiative pushes businesses of all sizes and sectors to adopt fundamental internet security practices, including using the Framework and similar risk management tools, engaging cybersecurity providers, and partnering with law enforcement before cyber incidents occur.

The Chamber has spearheaded some two dozen major regional roundtables and summits in Washington, D.C. Several regional events are taking place this year in the run-up to our 8th Annual Cybersecurity Summit on October 10, 2019. Both the Chamber and the FTC have made substantial commitments to business cyber education.[6]

STREAMLINING REGULATIONS IS JOB NO. 1

Positive elements of the rulemaking and the FTC's engagement with industry are only part of the picture. The Chamber is concerned that a number of the Commission's proposed modifications to the Safeguards Rule would conflict with our long-standing interest in fostering a dynamic cybersecurity governance model.

First, policymaking involves trade-offs. The agency's rulemaking elevates a more check-the-box approach to data security compared with the existing Safeguards Rule, which employs a more flexible model. A nonpartisan consensus exists indicating that industry and government need to better collaborate to meet the myriad challenges that face U.S. economic and national security.[7] The current Safeguards Rule is workable largely because it fits within the

mainstream of how the government and industry approach cybersecurity risk management across sectors.[8]

The Chamber contends that the Safeguards Rule should not be expanded to include additional requirements governing covered financial institutions' information security programs.[9] Ultimately, it is problematic that the FTC based its decision to amend the Safeguards Rule to include more specific security requirements on a comparatively limited subset of comments received from people and organizations in 2016.[10]

Second, the Chamber would have difficulty agreeing to an updated Safeguards Rule that does not grant strong legal liability and regulatory protections to covered entities. It is unclear whether the FTC can authorize robust protections on its own, or whether such actions would require an act of Congress.

What is noteworthy, Ohio enacted an innovative data security/cyber law in November 2018. The Ohio Data Protection Act (S.B. 220) grants an affirmative defense against data breach tort claims to those businesses that bring their cybersecurity frameworks up to an industry standard. Other states' data protection laws focus on requirements or penalties. The Ohio statute uses an affirmative defense to incentivize companies to improve their cyber practices.[11]

While the Chamber has not formally endorsed S.B. 220, the law could serve as a point of reference to possibly negotiate a national data security program. It combines businesses' usage of industry-recognized cyber frameworks with safeguards against legal liability. Further, the Chamber does not view the outcome of the Safeguards Rule update in isolation. Regulatory overreach by the agency would likely cast a shadow over other areas of cybersecurity where the FTC has authority, such as the Internet of Things (IoT).[12]

Third, policymakers should better balance the government's portion of the U.S. economic and national security burden to make the common refrain that cybersecurity is a shared public-private responsibility concrete. The Commission places, unintentionally, the defense of business information systems—particularly against nation state hackers, or their surrogates, as well as criminals—on the shoulders of the private sector. Still, businesses should not have to contend with top cyber threats alone, which is the stark reality today. Companies are in potential jeopardy with the FTC, in part, because foreign hackers are breaching U.S. networks with the direct or indirect support of nation states.[13]

Complicating matters, businesses are frustrated that they are often victimized twice—first, by the malicious actor(s); and second, by the court of public opinion.[14] To be sure, the Chamber wants private entities to vigorously mitigate threats to their assets and data, but victim-shaming leads to outcomes that are powerfully counterproductive to U.S. collective defense. In our experience, a number of cyberattacks against firms (or cities or government agencies) go unnoticed or unattributed because victims hesitate to share them with industry peers or government authorities because of the ensuing public backlash.[15]

Regulation and enforcement actions alone won't enhance private sector cybersecurity. Bad actors need to be deterred and reap the consequences of their actions—including for

justice's sake and to minimize the public-private challenges that arise from inadequate sharing and pushback against hackers.[16] Some semblance of fairness matters. Companies that suffer breaches should not come in for more punishment than the perpetrators.

Fourth, and most pressing, the Chamber urges the Commission and other policymaking bodies to collaborate with industry to streamline the nearly countless data security/cybersecurity regulations, not increase them. For several years, the Chamber has urged agency officials and lawmakers to work toward reducing duplicative and overly burdensome information security requirements that impact regulated institutions. To illustrate the point, a U.S. technology company executive recently shared with us that his firm must comply with approximately 750 data security/cyber regulations globally. And about one-third of these mandates are changing at any given time, he said.

The FTC should forgo moving forward on the rulemaking unless it can articulate a reasonable plan to help harmonize the myriad regulations that affect industry at the state, federal, and international levels vis-à-vis the Safeguards Rule proposal. Given the interconnected nature of the cyber regulatory landscape, this task would be difficult to do, but it is necessary.[17]

The Chamber further believes that expanding the regulation—whether in terms of imposing new requirements on already regulated entities or widening it to cover new ones—would impose additional costs and mandates on companies that we are unable to support. Some private organizations can absorb the added costs, while others cannot. Equally troublesome, the proposed requirements would increasingly divert company resources toward compliance and away from risk management activities that are tailored to businesses' unique security needs.

In sum, the Chamber is not yet convinced that enlarging the Safeguards Rule is necessary to achieve the FTC's mission, or that it would better shore up U.S. data security and/or cyber objectives. We urge the Commission to refrain from modifying the Safeguards Rule. However, if the FTC proceeds with its rulemaking, the Chamber's key recommended edits to the proposal are in the attachment (pages 5–14).

If you have any questions or need more information, please do not hesitate to contact Christopher Roberti (croberti@uschamber.com, 202-463-3100) or Matthew Eggers (meggers@uschamber.com, 202-463-5619).

Sincerely,

Christopher D. Roberti
Chief of Staff
Senior Vice President, Cyber, Intelligence, and Security

Matthew J. Eggers
Vice President, Cybersecurity Policy

***

RECOMMENDING CHANGES TO THE FTC'S PROPOSED RULEMAKING

The Chamber does not support changing the Safeguards Rule. However, we want to draw the Commission's attention to our recommended revisions to its proposal, which are provided in the comment boxes and green/underlined text (i.e., the latter are text additions). The blue/underlined text represents the Chamber's redline of how the FTC plans to amend 16 CFR part 314.[18]

PART 314—STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION[19]

Contents

Authority: 15 U.S.C. 6801(b), 6805(b)(2).[20]

~~Source: 67 FR 36493, May 23, 2002, unless otherwise noted.~~

§314.1 Purpose and scope.

(a) *Purpose*. This part, which implements sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act, sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

(b) *Scope*. This part applies to the handling of customer information by all financial institutions over which the Federal Trade Commission ("FTC" or "Commission") has jurisdiction. Namely, ~~T~~this part ~~refers to such entities~~ applies to those "financial institutions" over which the Commission has rulemaking authority pursuant to section 501(b) of the Gramm-Leach-Bliley Act. An entity is a "financial institution" if its business is engaging in an activity that is financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. 1843(k), which incorporates by reference activities enumerated by the Federal Reserve Board in 12 CFR 225.28 and 12 CFR 225.86. The "financial institutions" subject to the Commission's enforcement authority are those that are not otherwise subject to the enforcement authority of another regulator under Section 505 of the Gramm-Leach-Bliley Act, 15 U.S.C. 6805. More specifically, those entities include, but are not limited to, mortgage lenders, "pay day" lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, investment advisors that are not required to register

with the Securities and Exchange Commission, and entities acting as finders. They are referred to in this part as "~~y~~You." This part applies to all customer information in your possession, regardless of whether such information pertains to individuals with whom you have a customer relationship, or pertains to the customers of other financial institutions that have provided such information to you.

§314.2 Definitions.

(a) *In general.* Except as modified by this part or unless the context otherwise requires, the terms used in this part have the same meaning as set forth in the Commission's rule governing the Privacy of Consumer Financial Information, 16 CFR part 313.

(b) *Authorized user* means any employee, contractor, agent, or other person that participates in your business operations and is authorized to access and use any of your information systems and data.

(c) Security event means an event resulting in unauthorized access to, or disruption or misuse of, an information system or information stored on such information system.

(~~b~~d) *Customer information* means any record containing nonpublic personal information, as defined in 16 CFR 313.3(n),[21] about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.

(e) *Encryption* means the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key.

(f)(1) *Financial institution* means any institution the business of which is engaging in an activity that is financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. 1843(k). An institution that is significantly engaged in financial activities, or significantly engaged in activities incidental to such financial activities, is a financial institution.

(2) *Examples of financial institutions*. (i) A retailer that extends credit by issuing its own credit card directly to consumers is a financial institution because extending credit is a financial activity listed in 12 CFR 225.28(b)(1) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F), and issuing that extension of credit through a proprietary credit card demonstrates that a retailer is significantly engaged in extending credit.

(ii) An automobile dealership that, as a usual part of its business, leases automobiles on a nonoperating basis for longer than 90 days is a financial institution with respect to its leasing business because leasing personal property on a nonoperating basis where the initial term of the lease is at least 90 days is a financial activity listed in 12 CFR 225.28(b)(3) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(iii) A personal property or real estate appraiser is a financial institution because real and personal property appraisal is a financial activity listed in 12 CFR 225.28(b)(2)(i) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(iv) A career counselor that specializes in providing career counseling services to individuals currently employed by or recently displaced from a financial organization, individuals who are seeking employment with a financial organization, or individuals who are currently employed by or seeking placement with the finance, accounting or audit departments of any company is a financial institution because such career counseling activities are financial activities listed in 12 CFR 225.28(b)(9)(iii) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(v) A business that prints and sells checks for consumers, either as its sole business or as one of its product lines, is a financial institution because printing and selling checks is a financial activity that is listed in 12 CFR 225.28(b)(10)(ii) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(vi) A business that regularly wires money to and from consumers is a financial institution because transferring money is a financial activity referenced in section 4(k)(4)(A) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(A), and regularly providing that service demonstrates that the business is significantly engaged in that activity.

(vii) A check cashing business is a financial institution because cashing a check is exchanging money, which is a financial activity listed in section 4(k)(4)(A) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(A).

(viii) An accountant or other tax preparation service that is in the business of completing income tax returns is a financial institution because tax preparation services is a financial activity listed in 12 CFR 225.28(b)(6)(vi) and referenced in section 4(k)(4)(G) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(G).

(ix) A business that operates a travel agency in connection with financial services is a financial institution because operating a travel agency in connection with financial services is a financial activity listed in 12 CFR 225.86(b)(2) and referenced in section 4(k)(4)(G) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(G).

(x) An entity that provides real estate settlement services is a financial institution because providing real estate settlement services is a financial activity listed in 12 CFR 225.28(b)(2)(viii) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(xi) A mortgage broker is a financial institution because brokering loans is a financial activity listed in 12 CFR 225.28(b)(1) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(xii) An investment advisory company and a credit counseling service are each financial institutions because providing financial and investment advisory services are financial activities referenced in section 4(k)(4)(C) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(C).

(xiii) A company acting as a finder in bringing together one or more buyers and sellers of any product or service for transactions that the parties themselves negotiate and consummate is a financial institution because acting as a finder is an activity that is financial in nature or incidental to a financial activity listed in 12 CFR 225.86(d)(1).

(3) *Financial institution* does not include:

(i) Any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act (7 U.S.C. 1 *et seq.*);

(ii) The Federal Agricultural Mortgage Corporation or any entity chartered and operating under the Farm Credit Act of 1971 (12 U.S.C. 2001 *et seq.*);

(iii) Institutions chartered by Congress specifically to engage in securitizations, secondary market sales (including sales of servicing rights) or similar transactions related to a transaction of a consumer, as long as such institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party other than as permitted by sections 313.14 and 313.15; or

(iv) Entities that engage in financial activities but that are not significantly engaged in those financial activities, and entities that engage in activities incidental to financial activities but that are not significantly engaged in activities incidental to financial activities.

(4) *Examples of entities that are not significantly engaged in financial activities.*

(i) A retailer is not a financial institution if its only means of extending credit are occasional "lay away" and deferred payment plans or accepting payment by means of credit cards issued by others.

(ii) A retailer is not a financial institution merely because it accepts payment in the form of cash, checks, or credit cards that it did not issue.

(iii) A merchant is not a financial institution merely because it allows an individual to "run a tab."

(iv) A grocery store is not a financial institution merely because it allows individuals to whom it sells groceries to cash a check, or write a check for a higher amount than the grocery purchase and obtain cash in return.

(~~e~~g) *Information security program* means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

(h) *Information system* means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental controls systems.

(i) *Multi-factor authentication* means authentication through verification of at least two of the following types of authentication factors:

(1) Knowledge factors, such as a password;

(2) Possession factors, such as a token or text message on a mobile phone; or

(3) Inherence factors, such as biometric characteristics.

[Add lower-case letter.] *Sensitive customer information* means nonpublic electronic customer information which because of name, number, personal mark, or other identifier can be used to identify such customer, in combination with any one or more of the following data elements: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records.

(j) *Penetration testing* means a test methodology in which assessors attempt to circumvent or defeat the security features of an information system by attempting penetration of databases or controls from outside or inside your information systems.

(~~d~~k) *Service provider* means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to this part.

§314.3 Standards for safeguarding customer information.

(a) *Information security program.* You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. ~~Such safeguards~~The information security program shall include the

Commented [EMJ1]: The U.S. Chamber of Commerce recommends adding the wording, "or text message on a mobile phone," to make it consistent with section 500.01(f)(2) of the New York State Department of Financial Services Cybersecurity Regulation (DFS Cybersecurity Regulation). www.dfs.ny.gov/industry_guidance/cybersecurity

The Federal Trade Commission (FTC or the Commission) says that it plans to deviate from the DFS Cybersecurity Regulation (*Federal Register* 13164, footnote 74), citing National Institute of Standards and Technology guidelines. Yet the Chamber, like New York state regulators, believes that SMS text messages can be leveraged by businesses in practical and secure ways.

Commented [EMJ2]: The Chamber recommends adding "sensitive customer information" to the definitions list to appropriately narrow the scope of customer information that would be covered by the proposed rule. This definition would be consistent with section 500.01(g)(2) of the DFS Cybersecurity Regulation.

elements set forth in ~~§~~section 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

(b) *Objectives.* The objectives of section 501(b) of the Act, and of this part, are to:

(1) Insure the security and confidentiality of customer information;

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

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

§314.4 Elements.

In order to develop, implement, and maintain your information security program, you shall:

(a) Designate a qualified individual responsible for overseeing and implementing your information security program and enforcing your information security program (for purposes of this part, "Chief Information Security Officer" or "CISO"). The CISO may be employed by you, an affiliate, or a service provider. To the extent this requirement is met using a service provider or an affiliate, you shall:

(1) Retain responsibility for compliance with this part;

(2) Designate a senior member of your personnel responsible for direction and oversight of the CISO; and

~~(a) Designate an employee or employees to coordinate your~~(3) Require the service provider or affiliate to maintain an information security program that protects you in accordance with the requirements of this Part.

(b) Base your information security program on a risk assessment that ~~i~~identif~~y~~ies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks. ~~At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:~~

(1) ~~Employee training and management;~~The risk assessment shall be written and shall include:

~~(2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and~~

~~(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.~~

(i) Criteria for the evaluation and categorization of identified security risks or threats you face;

Commented [EMJ3]: The required designation of a CISO would likely require hiring a cybersecurity professional or a managed service provider. While such actions could improve a financial institution's cyber fitness, it is not an inexpensive undertaking. What is more, the supply of qualified cyber professionals in the market is widely known to be limited.

Commented [EMJ4]: The Chamber questions that a financial institution's information security program would be sufficiently risk based under this provision The specificity called for in the written risk assessment strikes us as rather prescriptive compared with the original wording of section 314.4(b).

(ii) Criteria for the assessment of the confidentiality, integrity, and availability of your information systems and customer information, including the adequacy of the existing controls in the context of the identified risks or threats you face; and

(iii) Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks.

(2) You shall periodically perform additional risk assessments that reexamine the reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and reassess the sufficiency of any safeguards in place to control these risks.

(c) Design and implement ~~information~~ safeguards to control the risks you ~~identity~~ [*sic*] identify through risk assessment, ~~and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.~~[See (d)(1) below.]including:

(1) Place access controls on information systems, including controls to authenticate and permit access only to authorized individuals, designed to protect against the unauthorized acquisition of customer information and to periodically review such access controls;

(2) Identify and manage the data, personnel, devices, systems, and facilities that enable you to achieve business purposes in accordance with their relative importance to business objectives and your risk strategy;

(3) Restrict access at physical locations containing customer information only to authorized individuals;

(4) Protect by encryption all sensitive customer information held or transmitted by you both in transit over external networks and at rest. To the extent you determine that encryption of sensitive customer information, either in transit over external networks or at rest, is infeasible, you may instead secure such sensitive customer information using effective alternative compensating controls reviewed and approved by your CISO;

(5) Adopt secure development practices for in-house developed applications utilized by you for transmitting, accessing, or storing sensitive customer information and procedures for evaluating, assessing, or testing the security of externally developed applications you utilize to transmit, access, or store sensitive customer information;

(6) Implement multi-factor authentication for any individual accessing customer information. Multi-factor authentication shall be utilized for any individual accessing your internal networks that contain customer information, unless your CISO has approved in writing the use of reasonably equivalent or more secure access controls;

Commented [EMJ5]: The FTC likely intended to write "identify."

Commented [EMJ6]: The Chamber believes that the word "designed" should be added to clarify that the controls are designed to accomplish the stated goals.

Commented [EMJ7]: The Commission's push for encrypting "all customer information" is based on the DFS Cybersecurity Regulation.

The Chamber noted to New York officials in 2016 that encryption is not practical in every circumstance. While we support strong encryption, mandating the encryption of all customer information is simply not practicable and would interfere with the legitimate operations of regulated companies.

Requiring covered entities to encrypt all customer information would constitute a costly and technical undertaking. Encryption is not a realistic solution to stronger information security in every situation.

See the Chamber's (et al.) 2016 letter to New York state regulators, which is available at www.uschamber.com/sites/default/files/group_letter_nysdfs_cyber_requirements.final_.pdf.

Commented [EMJ8]: The word "sensitive" is added three times to this subsection in keeping with the Chamber's recommendation to include a definition for "sensitive customer information" in the proposed rule.

Commented [EMJ9]: The word "sensitive" is added twice to this subsection.

Commented [EMJ10]: The Chamber believes that subsection (6) should be rewritten as follows to enhance clarity for readers/users:

"Implement multi-factor authentication for any individual accessing sensitive customer information on your internal network when connecting from an external network. In addition, based on the risk assessments performed under paragraph (b)(2) of the this section, implement multi-factor authentication to protect against unauthorized access to sensitive customer information, unless your CISO has approved in writing the use of alternative compensating controls."

In addition, the Chamber urges the FTC to clarify that multi-factor authentication does not apply to the internal access of customer information by a business' personnel. Network operators already apply security controls to validate internal users.

(7) Include audit trails within the information security program designed to detect and respond to security events;

(8) Develop, implement, and maintain procedures for the secure disposal of customer information in any format that is no longer necessary for business operations or for other legitimate business purposes, except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained;

(9) Adopt procedures for change management; and

(10) Implement policies, procedures and controls designed to monitor the activity of authorized users and detect unauthorized access or use of, or tampering with, sensitive customer information by such users.

(d)(1) Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems.

(2) The monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments. Absent effective continuous monitoring or other systems to detect, on an ongoing basis, changes in information systems that may create vulnerabilities, you shall conduct:

i. Annual penetration testing of your information systems determined each given year based on relevant identified risks in accordance with the risk assessment; and

ii. Biannual vulnerability assessments, including any systemic scans or reviews of information systems reasonably designed to identify publicly known security vulnerabilities in your information systems based on the risk assessment.

(e) Implement policies and procedures to ensure that personnel are able to enact your information security program by:

(1) Providing your personnel with security awareness training that is updated to reflect risks identified by the risk assessment;

(2) Utilizing qualified information security personnel employed by you or an affiliate or service provider sufficient to manage your information security risks and to perform or oversee the information security program;

(3) Providing information security personnel with security updates and training sufficient to address relevant security risks; and

(4) Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.

(~~d~~f) Oversee service providers, by:

Commented [EMJ11]: The word "sensitive" is added once to this subsection.

Commented [EMJ12]: The Chamber agrees that protecting sensitive business and consumer data is central to most robust cybersecurity programs. Yet, as written, this section's requirements are overly generalized. FTC-regulated parties should be allowed to craft a testing program based on its perceived risk environment.

The Chamber believes that cyber programs must be flexible to enable entities to adapt their defenses and measures to address existing threats, which constantly evolve. The proposal should be amended to clearly recognize each entity's special risk profile.

Commented [EMJ13]: The FTC's rulemaking would require security personnel to attend regular cybersecurity awareness training sessions, which seems sensible on the surface.

The Chamber supports greater cybersecurity awareness among businesses for employee education. But, in practice, the training sessions could become rigid, unenthusiastic exercises that dictate specific roles and responsibilities for companies' personnel.

Commission mandates could easily negate financial firms' discretion about training and spread thinly the resources they need to adapt to a changing threat environment. Businesses are in the best position, working collaboratively with government officials, to understand how personnel need to be trained and monitored.

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue~~; and~~

(2) Requiring your service providers by contract to implement and maintain such safeguards~~.~~; and

(3) Periodically assessing your service providers based on the risk they present and the continued adequacy of their safeguards.

(~~e~~g) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (~~c~~d) of this section; any material changes to your operations or business arrangements; the results of risk assessments performed under paragraph (b)(2) of this section; or any other circumstances that you know or have reason to know may have a material impact on your information security program~~.~~;

(h) Establish a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of sensitive customer information in your possession. Such incident response plan shall address the following areas:

(1) The goals of the incident response plan;

(2) The internal processes for responding to a security event;

(3) The definition of clear roles, responsibilities and levels of decision-making authority;

(4) External and internal communications and information sharing;

(5) Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;

(6) Documentation and reporting regarding security events and related incident response activities; and

(7) The evaluation and revision as necessary of the incident response plan following a security event.

(i) Require your CISO to report in writing, at least annually, to your board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a senior officer responsible for your information security program. The report shall include the following information:

(1) The overall status of the information security program and your compliance with this Rule; and

(2) Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider

Commented [EMJ14]: The word "sensitive" is added once to this subsection.

Commented [EMJ15]: This subsection calls for regulated businesses to remediate "*any* identified weaknesses" in information systems and associated controls [italics added]. Such thinking, on the surface, seems logical but is out of step with managing risk based on prioritizing threats. Companies that must remediate all weaknesses equally could end up inadequately fixing the ones that matter most.

arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program.

§314.5 Effective date.

~~(a) Each financial institution subject to the Commission's jurisdiction must implement an information security program pursuant to this part no later than May 23, 2003.~~

~~(b) Two-year grandfathering of service contracts. Until May 24, 2004, a contract you have entered into with a nonaffiliated third party to perform services for you or functions on your behalf satisfies the provisions of §314.4(d), even if the contract does not include a requirement that the service provider maintain appropriate safeguards, as long as you entered into the contract not later than June 24, 2002.~~

Sections 314.4(a), 314.4(b)(1), 314.4(c)(1)-(10), 314.4(d)(2), 314.4(e), 314.4(f)(3), 314.4(h), and 314.4(i) are effective as of [six months after publication of the final rule].

§314.6 Exceptions.

Sections 314.4(b)(1), 314.4(d)(2), 314.4(h), and 314.4(i) do not apply to financial institutions that maintain customer information concerning fewer than five thousand consumers.

Endnotes

[1] The Federal Trade Commission (FTC), "Standards for Safeguarding Customer Information," *Federal Register* (April 4, 2019). www.federalregister.gov/documents/2019/04/04/2019-04981/standards-for-safeguarding-customer-information

[2] *Federal Register*, page 13169.

[3] See "U.S. Chamber Privacy Principles" (September 6, 2018). www.uschamber.com/issue-brief/us-chamber-privacy-principles

[4] *Federal Register*, pages 13158, 13160.

[5] *Federal Register*, page 13177.

[6] See Federal Communications Commission, FTC, and U.S. Chamber of Commerce cybersecurity resources for small and midsize businesses.

- www.fcc.gov/general/cybersecurity-small-business
- www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity
- www.uschamber.com/CybersecurityEssentials

[7] In September 2016, former-Commerce Secretary Pritzker addressed the Chamber on cybersecurity. First, the secretary stressed that cyberattacks cannot be handled solely by the U.S. government. Yet cyberspace is the "only domain where we ask private companies to defend themselves" against foreign powers and other significant threats. She wondered aloud, "Does that sound as crazy to you as it does to me?" Second, Pritzker noted that federal laws and regulations are unable to keep pace with rapidly evolving cyber threats. "No static checklist, no agency rule, no reactive regulation is capable of thwarting a threat we cannot foresee." A core problem, she observed, is that

relationships between businesses and regulators are "inherently adversarial," not collaborative, and this inhibits sound security.
www.uschamber.com/sites/default/files/oct_20._letter_to_wh_cyber_commission_re_sec_pritzker_address_final.pdf

[8] See the Chamber's September 2016 and July 2016 letters, respectively, to the Commission on Enhancing National Cybersecurity and the Cybersecurity Forum for Independent and Executive Branch Regulators (the Cyber Forum). We called on policymakers to help agencies harmonize existing regulations with the Cybersecurity Framework and maintain the Framework's voluntary nature.

The Chamber added that some government entities are forming genuine partnerships with industry to enhance the security and resilience of U.S. critical infrastructure; some agencies are seemingly exploring ways to flex their regulatory muscles; and some federal bodies are apparently abandoning the spirit, if not the precepts, of the 2013 cybersecurity executive order and the Cybersecurity Enhancement Act of 2014 (P.L. 113-274). Both measures call for modernizing cyber rules.
www.uschamber.com/sites/default/files/u.s._chamber._letter_nist-wh_cyber_commission_rfi_sept._9_final_v2.1.pdf
www.uschamber.com/sites/default/files/u.s._chamber_letter_to_cyber_forum_july_8.final_.pdf

[9] The Chamber made similar points to the FTC in 2016. We agree with many of the dissenting arguments put forth by Commissioners Joshua Phillips and Christine Wilson. *Federal Register*, pages 13176–13177.
www.ftc.gov/system/files/documents/public_comments/2016/11/00022-129360.pdf

[10] *Federal Register*, pages 13159–13160.

[11] Columbus Chamber of Commerce event, "Ohio's New Cybersecurity Law: What Will It Mean for Business and for Data Protection?" (May 10, 2019).

- https://columbus.org/events/ohios-new-cybersecurity-law-what-will-it-mean-for-business-and-for-data-protection-2
- www.legislature.ohio.gov/legislation/legislation-summary?id=GA132-SB-220
- https://moritzlaw.osu.edu/data-and-governance/wp-content/uploads/sites/105/2019/03/cybersecurity-whitepaper-32819F-1.pdf
- http://allforohio.com/2018/08/29/ohio-enacts-law-acknowledging-blockchain-transaction-granting-safe-harbor-protections-to-eligible-business-from-data-breach-claims

[12] In April 2019, the Chamber testified before the Senate Commerce Committee Security Subcommittee on strengthening the cybersecurity of the Internet of Things (IoT), arguing that federal preemption is needed to harmonize the expanding policy and regulatory fragmentation that is taking place domestically and overseas. We said a fragmented cyber environment creates uncertainty for device makers and buyers and splinters the resources that businesses devote to sound device development, production, and assessments.

The Chamber is urging the Senate Commerce Committee to consider legislation that would spur device makers to build to an industry-led core IoT cyber baseline, while granting legal liability and regulatory protections to the makers and sellers of strong IoT equipment. The Chamber is concerned a regulatory response by the Commission would represent a trend toward prescriptive standards-setting that would augur poorly for public-private cooperation regarding IoT cybersecurity.
www.commerce.senate.gov/public/index.cfm/2019/4/strengthening-the-cybersecurity-of-the-internet-of-things

[13] Foreign hacking against the U.S. business community is well documented. See, for example, Tim Mauer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, U.K.: Cambridge Univ. Press, 2018).

[14] Matt Reynolds, "Self-defense in cyberspace would put businesses at risk, experts say," *MarketWatch* (July 27, 2019). The Chamber said that H.R. 3270, the Active Cyber Defense Certainty Act, sponsored by Rep. Tom Graves (R-GA), is borne of industry "frustration" with foreign hacking that goes mostly unpunished. The Chamber has not taken a position on this legislation but believes that it spurs a necessary debate on a key policy issue.
www.marketwatch.com/story/self-defense-in-cyberspace-would-put-businesses-at-risk-experts-say-2019-07-25?mod=hp_econ

https://tomgraves.house.gov/news/documentsingle.aspx?DocumentID=401122

[15] See the Chamber's July 2016 letter to the Cyber Forum. We said that companies hacked by foreign governments and criminal groups often face unwarranted blame, including shouldering disproportionate burdens for deterrence and liability. Governments should reject a blame the victim mentality when it comes to cyber intrusions. The Chamber agrees with former-Assistant Attorney General for National Security John Carlin who said, "Blaming companies for sophisticated breaches by nation states is akin to blaming a pedestrian who gets stabbed by a stranger for simply making eye contact beforehand."
www.uschamber.com/sites/default/files/u.s._chamber_letter_to_cyber_forum_july_8.final_.pdf

[16] The Chamber especially refers to cyber activity that is sponsored by Russia, China, Iran, and North Korea against covered financial institutions and other private entities. Defense Science Board, *Task Force on Cyber Deterrence* (Washington, D.C.: Department of Defense, February 2017).
www.acq.osd.mil/dsb/reports/2010s/dsb-cyberdeterrencereport_02-28-17_final.pdf

Keir Giles and Andrew Monaghan, *Legality in Cyberspace: An Adversary View* (Carlisle, PA: U.S. Army War College, March 2014). Russia, China, Iran, and North Korea have earned reputations as permissive environments for cybercrime and the theft of intellectual property targeting U.S. companies (pages 18–19).
https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1193

See, too, Daniel R. Coats, Director of National Intelligence, *Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community*. Senate Intelligence Committee hearing, "Worldwide Threats" (January 29, 2019).
www.odni.gov/index.php/newsroom/congressional-testimonies/item/1947-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community
www.intelligence.senate.gov/hearings/open-hearing-worldwide-threats

[17] The authors of the *Fifth Domain* articulate well the need to prune the regulatory bushes. They write:

> Although [the] Clinton, Bush, and Obama [administrations] eschewed, rejected, or declined to establish a [comprehensive] federal cybersecurity regulatory regime, *there is a mountain of cybersecurity regulation created by federal agencies*. Banks, nuclear power plants, self-driving cars, hospitals, insurance companies, defense contractors, passenger aircraft, chemical plants, and dozens of other private-sector entities are all subject to cybersecurity regulation by a nearly indecipherable stream of agencies including the FTC, FAA, DHS, DoD, FERC, DOE, HHS, DOT, OCC, and on and on. Variation in federal regulations should be a result of conscious policy choices, *not the incremental accretion of rules* written at different times with little central guidance. It is time to step back and assess which of these agencies and regulations have been effective [italics added].

Richard A. Clarke and Robert K. Knake, *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats* (New York: Penguin Press, 2019), pages 113–114.

[18] See, specifically, *Federal Register*, pages 13173–13176.

[19] www.govinfo.gov/app/details/CFR-2009-title16-vol1/CFR-2009-title16-vol1-part314

[20] www.govinfo.gov/app/details/USCODE-2011-title15/USCODE-2011-title15-chap94-subchapI-sec6801
www.govinfo.gov/content/pkg/USCODE-2015-title15/pdf/USCODE-2015-title15-chap94-subchapI-sec6805.pdf

[21] See Part 313, Privacy of Consumer Financial Information, particularly section 313.3 on definitions:

(n)(1) *Nonpublic personal information* means:
(i) Personally identifiable financial information; and
(ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.
(2) *Nonpublic personal information* does not include:

(i) Publicly available information, except as included on a list described in paragraph (n)(1)(ii) of this section; or

(ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any personally identifiable financial information that is not publicly available.

(3) *Examples of lists*—

(i) Nonpublic personal information includes any list of individuals' names and street addresses that is derived in whole or in part using personally identifiable financial information (that is not publicly available), such as account numbers.

(ii) Nonpublic personal information does not include any list of individuals' names and addresses that contains only publicly available information, is not derived, in whole or in part, using personally identifiable financial information that is not publicly available, and is not disclosed in a manner that indicates that any of the individuals on the list is a consumer of a financial institution.

www.govinfo.gov/app/details/CFR-2011-title16-vol1/CFR-2011-title16-vol1-sec313-3