U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

February 7, 2022

Via https://www.federalregister.gov

David Lincicum
Katherine McCarron
Robin Wetherill
Division of Privacy and Identity Protection
Bureau of Consumer Protection
Federal Trade Commission
Washington, D.C. 20580

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

Dear Mr. Lincicum, Ms. McCarron, and Ms. Wetherill:

The U.S. Chamber of Commerce appreciates the opportunity to comment on the Federal Trade Commission's (FTC's or the Commission's) proposed amendment to the Safeguards Rule on standards for safeguarding customer information. The FTC's December 9, 2021, notice would require "financial institutions" to report "any *security event* where the financial institutions have determined misuse of customer information has occurred or is reasonably likely and at least 1,000 consumers have been affected or reasonably may be affected" [italics added].[1]

In an August 2019 letter to the Commission on updates to the Safeguards Rule, the Chamber praised the FTC's decision not to promulgate a new reporting or notification requirement, which would duplicate or conflict with mandates that financial institutions are already subject to.[2] The decision was sound at the time, and it remains so today.

Key Points

- The Federal Trade Commission (FTC) and other policymaking bodies need to prioritize collaboration with industry to streamline the nearly countless cyber event or incident reporting regulations and not add to them.
- Many business sectors already have existing obligations to report cyber events or incidents to federal and/or state regulatory agencies. Despite this situation, Congress is preparing to pass mandatory cyber incident reporting legislation, and several federal agencies have recently finalized or are readying new reporting rules.
- Reporting regulations seem divorced from a concerted strategy that would turn a mass of cyber incident notifications into value-added security and trusted partnerships.
- The FTC should forgo moving forward on the security event rulemaking unless it can articulate a reasonable plan to harmonize the myriad regulations that affect industry at the state, federal, and international levels vis-à-vis the Safeguards Rule, among other related requirements.

STREAMLINING REPORTING REGULATIONS IS JOB NO. 1

The Chamber urges the Commission and other policymaking bodies to collaborate with industry to streamline the nearly countless data breach/data security/cybersecurity notification or incident reporting regulations, and not add to them. For many years, the Chamber has urged federal agency officials and lawmakers to work toward harmonizing duplicative and overly burdensome information security requirements that impact regulated institutions.

The FTC should forgo moving forward on the security event rulemaking unless it can articulate a reasonable plan to harmonize the myriad regulations that affect industry at the state, federal, and international levels vis-à-vis the Safeguards Rule, among many other requirements. Few organizations—public or private—have taken on the task of cataloging all the various reporting and/or notification requirements imposed on the private sector because doing so is quite daunting and ever-changing.

The Office of the Comptroller of the Currency, the Federal Reserve Board, and the Federal Deposit Insurance Corporation published a final rule in November 2021 on data breach reporting. It requires a banking organization to notify its primary federal regulator of any "computer-security incident" that rises to the level of a "notification incident" as soon as possible and no later than 36 hours. The rule also requires a bank service provider to notify each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a cyber incident that has caused, or is reasonably likely to cause, a material service disruption or degradation for 4 or more hours.[3]

Additionally, the Transportation Security Administration (TSA) issued an emergency security directive—which has the effect of a regulation— for pipeline cybersecurity last May. TSA Security Directive Pipeline-2021-01 requires regulated pipeline operators to report cybersecurity incidents, provide a cybersecurity coordinator to liaise with TSA and the Cybersecurity and Infrastructure Security Agency (CISA) "to coordinate cybersecurity practices and address any incidents that arise," review current activities against TSA voluntary guidelines, and implement mitigation measures and report results to TSA and CISA. A second directive issued in July 2021 elaborated on requirements in the first directive.[4]

What's more, the FTC, the Securities and Exchange Commission (SEC), and the Federal Communications Commission (FCC) intend to write new cyber reporting rules. Also, Congress is close to passing compulsory cyber incident reporting legislation.

First, in a speech delivered on January 24, 2022, SEC Chair Gary Gensler said that he has directed SEC staff to develop recommendations on how the SEC can "strengthen financial sector registrants' cybersecurity hygiene and incident reporting, taking into consideration guidance issued by CISA and others." Chair Gensler suggested that the SEC intends to revise companies' disclosure obligations, including when they make ransomware payments.[5]

Second, on January 12, 2022, FCC Chairwoman Jessica Rosenworcel announced that the FCC plans to promulgate a rule tied to notifying customers and federal law enforcement of breaches of customer proprietary network information. The proposal, Chairwoman Rosenworcel noted, would make several updates to the FCC's existing rules, including eliminating the current seven business day mandatory waiting period for notifying customers of a breach; expanding

customer protections by requiring notification of inadvertent breaches; and requiring carriers to notify the FCC of all reportable breaches, as well as the FBI and Secret Service.[6]

Third, cyber incident reporting legislation would require certain owners/operators of critical infrastructure to report "covered cyber incidents," which would be defined by CISA through a rulemaking, to CISA withing 72 hours. The legislation would also compel covered entities to report ransomware payments to CISA within 24 hours of making them.

The cyber incident reporting legislation would call on the national cyber director (NCD) to lead an intergovernmental Cyber Incident Reporting Council (CIRC) composed of the Office of Management and Budget, CISA, and sector risk management agencies (SRMAs) "to coordinate, deconflict, and harmonize Federal incident reporting requirements, including those issued through regulations, for covered entities." The bill would also task the NCD and the other federal agency officials to periodically review existing reporting requirements to avoid conflicting, duplicative, or burdensome requirements and streamline those reporting requirements, as well as submit a report to Congress.[7]

The Chamber appreciates the cyber incident reporting legislation's attention to harmonizing federal reporting requirements. We believe that the NCD should have authority to streamline reporting mandates in a manner that would not rely on persuasion but would be binding on federal agencies. Given the interconnected nature of the cyber regulatory landscape, harmonization—while difficult—is necessary.

It is particularly significant that the agency regulations and the legislation are uncoordinated at the federal level. Nor do they account for security breach laws across the 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands that require businesses to notify individuals of security breaches of information involving personally identifiable information.[8] Relatedly, the New York State Department of Financial Services requires entities that it oversees to notify the department "as promptly as possible but in no event later than 72 hours from a determination that a cybersecurity event has occurred."[9]

***

Among the Chamber's leading concerns with current and potentially new cyber reporting regimes is that several critical infrastructure sectors have existing obligations to report cyber incidents to federal and/or state regulatory agencies. The regulations seem divorced from any overarching strategy that would turn a likely mass of cyber incident reporting into value-added security and trusted public-private relationships. Indeed, quality intelligence comes not from coerced reporting of private entities but from the intentional cooperation of people persuaded that the government can effectively use the information to better protect them and U.S. institutions. None of the reporting requirements suggest that the federal government would take actions to disrupt or degrade the malicious actions of foreign countries or their proxies.

It is crucial that the administration, Congress, and industry partner on streamlining federal and state reporting requirements to ensure that industry resources are used efficiently to combat malicious cyber threats. Businesses should not be devoting limited resources to customizing reports on the same incident for multiple agencies. A single report to one federal agency should

suffice to meet legislative and regulatory mandates. Reporting should be made either to CISA or the appropriate SRMA, which should then disseminate reports to other relevant agencies.

PRELIMINARY FEEDBACK ON COMMISSION'S QUESTIONS

The remainder of this letter consists of business community feedback to some of the Commission's questions. The Chamber does not attempt to answer each question that the FTC asks. Our answers to the questions should not be construed to be an endorsement of the FTC's proposed security event rulemaking.

The information to be contained in any notice to the Commission. Is the proposed list of elements sufficient? Should there be additional information? Less?

The Chamber believes that the information submitted to the Commission should be as simple as possible to complete. According to the proposed rule, a notice would involve "a limited set of information," generally consistent with existing state breach notification requirements. Financial institutions would be required to provide the following information to the FTC:

- The name and contact information of the reporting financial institution.
- A description of the types of information involved in the security event.[10]
- The date or date range of the security event (if this information can be determined).
- A general description of the security event.

The Commission wants notices to be provided electronically through a form on the FTC's website. However, in situations where covered entities may lack access to the internet, perhaps owing to an outage, financial institutions should be able to report to the Commission via alternative means (e.g., a mailed hard copy).

Whether the Commission's proposed threshold for requiring notice—for those security events for which misuse of the information of 1,000 or more consumers has occurred or is reasonably likely to occur—is the appropriate one. What about security events in which misuse is possible but not likely? Should there be a carve-out for security events solely involving encrypted data?

It is unclear from the proposed rule what the definition of "misuse" is. Misuse could have multiple meanings in ordinary use.

Yes, the FTC should create a carve-out from the proposed requirement for encrypted data.

The timing for notification to be given to the Commission. Is the current proposal of a maximum of 30 days after discovery of the security event reasonable? Is a shorter period practicable?

The Chamber believes that financial institutions should be granted at least 30 days to notify the Commission after *confirmation* of a security event by a financial institution. Businesses need clarity in reporting requirements, which should be targeted to well-defined and confirmed security events. Some policy and legislative language that we have considered, including "discovery," can be overly subjective. A reportable security event should be attached to clear, objective criteria whether a security event is considered by policymakers in a rulemaking or legislation.[11]

Whether the requirement should allow law enforcement agencies to prevent or delay notification if notification to the Commission would affect law enforcement investigations. The proposed rule does not include such a requirement. Comments are also welcome on whether such a law enforcement right to prevent or delay notification is only necessary to the extent notices are made public.

The FTC's proposed rule should allow for a reporting delay per a request from law enforcement if the affected financial institution gives its consent to authorities. The proposed rule should also allow a reporting delay if contractual obligations would require informing another party of the notification to the government, but law enforcement deems that informing the other party is undesirable or inadvisable based on the circumstances of the investigation.

Whether the information reported to the Commission should be made public. Should the Commission permit affected financial institutions to request confidential treatment of the required information? If so, under what circumstances? Should affected financial institutions be allowed to request delaying the public publication of the security event information and, if so, on what basis?

The Chamber strongly believes that information submitted to the Commission should not be publicly disclosed. We believe that Congress should authorize protections for financial institutions under the proposed rule that are found in legislation like the Cybersecurity Information Sharing Act of 2015 and/or key cyber incident reporting bills.[12]

Whether instead of implementing a stand-alone reporting requirement, the Commission should only require notification to the Commission whenever a financial institution is required to provide notice of a security event or similar to a governmental entity under another state or federal statute, rule, or regulation. How would such a provision affect the Commission's ability to enforce the rule? Would such an approach affect the burden on financial institutions? Would such an approach generate consistent reporting due to differences in applicable laws? Whether a notification requirement should be included at all.

The Chamber urges the Commission to avoid creating another data breach/data security/cybersecurity notification or reporting requirement on businesses. Congress and agencies are developing more laws and regulations without stitching them together in a way that is intelligible to the private parties that must implement them.

Agencies must do a better job of treating reporting as a means to bidirectional sharing and collaboration. Cybersecurity information sharing must be bidirectional. Information reported to an agency needs to be promptly aggregated, anonymized, analyzed, and shared with industry to foster the mitigation and prevention of future cyber incidents. A persistent shortcoming experienced by businesses across many sectors is a lack of timely and effective action or feedback on cyber reports from government. The Chamber wants policies and outcomes that lead to businesses telling us that they are receiving actionable data and assistance from CISA, law enforcement, and other agencies to enhance industry groups' security postures.

The Chamber welcomes the opportunity to provide the FTC with comments on the proposed security event rule. 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
Senior Vice President
Cyber, Intelligence, and
and Supply Chain Security

Matthew J. Eggers
Vice President
Cybersecurity Policy

Notes

---

[1] https://www.federalregister.gov/documents/2021/12/09/2021-25064/standards-for-safeguarding-customer-information

[2] The Federal Trade Commission (FTC), "Standards for Safeguarding Customer Information," *Federal Register* 13169, April 4, 2019.
www.federalregister.gov/documents/2019/04/04/2019-04981/standards-for-safeguarding-customer-information

See the U.S. Chamber of Commerce's August 2, 2019, comment letter to the FTC.
https://www.regulations.gov/comment/FTC-2019-0019-0033

[3] The Office of the Comptroller of the Currency, the Federal Reserve Board, and the Federal Deposit Insurance Corporation, "Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, *Federal Register*, November 23, 2021.
https://www.federalregister.gov/documents/2021/11/23/2021-25510/computer-security-incident-notification-requirements-for-banking-organizations-and-their-bank

[4] Congressional Research Service (CRS), *Critical Infrastructure Risk Management: Securing the Oil and Gas Supply Chain*, December 13, 2021, p. 23.
https://crsreports.congress.gov/product/pdf/R/R46987

[5] Securities and Exchange Commission (SEC), "Cybersecurity and Securities Laws," January 24, 2022.
https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124?utm_medium=email&utm_source=govdelivery

[6] Federal Communications Commission (FCC), "Chair Rosenworcel Circulates New Data Breach Reporting Requirements," January 12, 2022.
https://www.fcc.gov/document/chair-rosenworcel-circulates-new-data-breach-reporting-requirements

It is important to note that cyber incident reporting legislation does not safeguard industry reports submitted to law enforcement. The Chamber believes that cyber incident reporting to law enforcement should be protected from legal liability, public disclosure, among other considerations.

[7] See section 6104 of S. 2875, the Cyber Incident Reporting Act of 2021, as found in the November 18, 2021, *Congressional Record*, S8486.
https://www.congress.gov/117/crec/2021/11/18/167/201/CREC-2021-11-18-senate.pdf

[8] See National Council of State Legislatures, "Security Breach Notification Laws." Last updated on January 17, 2022, at the time of this writing.
https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

[9] 23 CRR-NY 500.17.
https://www.dfs.ny.gov/industry_guidance/cybersecurity

[10] According to the FTC, a "security event" refers to "an event resulting in unauthorized access to, or disruption or misuse of, an information system, information stored on such information system, or customer information held in physical form." 16 CFR § 314.2(p).
https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314

[11] See the October 4, 2021, coalition letter on cyber incident reporting that was sent to the members of the Senate Homeland Security and Governmental Affairs Committee, the Senate Intelligence Committee, and the House Homeland Security Committee.
https://www.uschamber.com/security/cybersecurity/coalition-letter-cyber-incident-reporting

[12] For more information on the Cybersecurity Information Sharing Act of 2015 (CISA 2015), see title N of H.R. 2029, the Consolidated Appropriations Act, 2016 (P.L. 114-113).
https://www.congress.gov/bill/114th-congress/house-bill/2029

S. 2875, the Cyber Incident Reporting Act of 2021.
https://www.congress.gov/bill/117th-congress/senate-bill/2875

H.R. 5440, the Cyber Incident Reporting for Critical Infrastructure Act of 2021.
https://www.congress.gov/bill/117th-congress/house-bill/5440

Last year, the Chamber worked closely with House and Senate lawmakers on cyber incident reporting legislation (i.e., S. 2875 and H.R. 5440). Several policy objectives that we urged bill writers to adopt could apply in part, if not fully, to the FTC's security event rulemaking:

> The legislation should establish that the act of reporting a covered incident [to the Cybersecurity and Infrastructure Security Agency] and the contents of any report, including supplemental reporting, are protected from legal liability. Information contained in notifications should not be subject to discovery in any civil or criminal action. Reporting entities, in essence, should not be penalized after the fact for complying with a legal obligation. In addition, bill writers are urged to aggressively limit the amount of information that covered entities would be required to submit to CISA or their relevant sector regulator.
>
> Legislation needs to limit the use of information that is provided to the government pursuant to the law. Restrictions on government use of data should closely align with CISA 2015, which contains provisions to exempt reported information from federal and state disclosure laws and regulatory use; treat shared information as commercial, financial, and proprietary; waive governmental rules related to ex parte communications; and preserve trade secret protections and any related privileges or protections.