May 9, 2022

Submitted electronically via rule-comment@sec.gov

The Honorable Vanessa A. Countryman
Secretary, Securities and Exchange Commission
100 F Street NE
Washington, DC 20549

Re: National Restaurant Association Comments on 17 CFR Parts 229, 232, 239, 240, and 249 [Release Nos. 33-11038; 34-94382; IC-34529; File No. S7-09-22]

Dear Secretary Countryman,

On behalf of the National Restaurant Association, thank you for the opportunity to comment on the Notice of Proposed Rulemaking (or "Proposed Rules") regarding Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure issued by the Securities and Exchange Commission ("SEC" or "Commission") published in the Federal Register on March 23, 2022.[1] While the Association supports reasonably timely and protected disclosures of cybersecurity incidents to the federal government, we oppose the Commission's proposed rules as drafted due to the duplicative nature of current and future cybersecurity legislation, the potential for creating additional harms to businesses resulting from premature disclosures, and the overly prescriptive requirements around risk management and governance strategy reporting. Because of these concerns we urge the Commission to rescind its proposal in its current form.

Founded in 1919, the National Restaurant Association ("the Association") is the leading business association for the restaurant and foodservice industry, representing more than 14.5 million employees, nearly 10 percent of the nation's workforce. As the nation's second-largest private sector employer, with nearly one million locations across the country, the restaurant industry is a vital driver of the U.S. economy.

While 90% of restaurants across the country have less than 50 total staff, restaurants of all cuisines and sizes routinely safeguard their most valuable assets. Whether it is putting cash and receipts in a register or safe, maintaining the highest standards when selecting, storing, and preparing food, or providing a safe and secure environment for customers and employees alike, protection is a priority for restaurant operators. Securing our customers' personal information is no different – operators work tirelessly to strengthen their cyber defenses to help avoid being victimized by threat actors because they recognize that data security is crucial to a restaurant's success in today's digital economy.

I. Harmonization of Potentially Duplicative or Conflicting Requirements Between Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), Other Data Breach Laws, and SEC's Proposed Rules

Earlier this year, as part of the $1.1 trillion spending package, Congress passed the Cybersecurity Incident Reporting for Critical Infrastructure Act (CIRCIA), which requires companies deemed to fall within a "critical infrastructure" sector to notify the Cybersecurity and Critical Infrastructure Agency (CISA) within 72 hours of a significant cyber incident and, in the case of ransomware, provide notification within 24 hours of making a payment.[2] The Association believes that CIRCIA represents an important step

[1] SEC's Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Proposed Rules
[2] *Consolidated Appropriations Act, 2022*

towards increasing federal government oversight of data security incidents, especially in the wake of last year's Executive Order 14028, "Improving the Nation's Cybersecurity," and the potential implications for American businesses resulting from the ongoing Russia-Ukraine conflict. However, CIRCIA does not identify which of the critical infrastructure sectors will be considered "covered entities," nor does it specify what will be considered a "covered cyber incident" under the law—these key definitions will be finalized as part of CISA's rulemaking process scheduled to take place over the course of the next two years.[3] Until these definitions can be agreed upon, the Association believes it will be challenging for the SEC to harmonize the potentially duplicative and/or conflicting reporting requirements between CIRCIA and its own proposal.

In addition to general ambiguities surrounding CIRCIA, companies must already comply with a wide array data breach and security incident reporting obligations at both the state and federal levels. Restaurants across the country are currently obligated to report cyber-related incidents under the Health Insurance Portability and Accountability Act (HIPAA) and the Children's Online Privacy Protection Act (COPPA), as well as comply with data breach laws in all 50 states. These varying state laws often contain "different requirements for determining whether a breach has occurred and for the notices that are required," meaning that "businesses must consider the scope of the data they collect and store in order to determine whether they are likely to have obligations to report under the laws of a given state."[4] In many cases, these state laws impose varying obligations for how and when to notify the identified individuals, Attorneys General offices, and relevant Credit Reporting Agencies.

While the SEC appears to acknowledge that companies may need to comply with many "data breach disclosure requirements… [that] may cover some of the material incidents that companies would need to report under the proposed amendments, but not all incidents,"[5] we believe the Commission does not fully appreciate how its proposed rules would further strain restaurants' and other businesses' limited resources to defend against malicious cyber-attacks while complying with the multitude of federal and state laws already on the books. Therefore, the Association urges the Commission to more clearly stipulate how it intends to harmonize this myriad of cybersecurity reporting regulations affecting the business community at all levels of government.

II. Reporting of Cybersecurity Incidents on Form 8-K Within 4 Business Days

Under its proposed rules, the Commission would amend Form 8-K to add Item 1.05 to require a company to disclose information about a cybersecurity incident within 4 business days after the company determines that it has experienced a "material" cybersecurity incident. The SEC argues that such reporting would "significantly improve the timeliness of cybersecurity incident disclosures, as well as provide investors with more standardized and comparable disclosures."[6]

While we appreciate the Commission's desire to collect more data from industry regarding the nature of the cyber threats they endure, the proposed 4-day notification timeline would be shorter than nearly all currently applicable data breach laws that restaurants currently comply with. As mentioned previously, CIRCIA provides a 72-hour notification regime but has not yet come into effect, while most states do not specify an exact timeframe for reporting a cyber-related incident—those that do generally prescribe a 30–45-day timeline for notification to a combination of affected individuals, Attorneys General offices, and other key reporting and law enforcement agencies.

In addition to this lack of harmonization, the Association is concerned that the Commission's proposed 4-day reporting timeframe could imperil a restaurant's cyber risk management strategy. Often there are

[3] *Consolidated Appropriations Act, 2022*
[4] https://www.burr.com/2021/12/10/data-breach-notification-laws-in-the-united-states-what-is-required-and-how-is-that-determined/
[5] SEC Proposed Rules
[6] SEC Proposed Rules

conflicting and competing priorities early in a cyber incident, and for restaurants and many other businesses, it is common for an incident response plan to take several weeks to determine when the incident was discovered; whether it is ongoing; whether any data was stolen, altered, accessed, or used for any other unauthorized purpose; the overall effect of the incident on the company's operations; and whether the company has remediated or is currently remediating the incident. Even with a perfectly operating team following a well-constructed incident response plan, a restaurant would be extremely hard pressed to meet the reporting requirements outlined in the Commission's proposed rules while also fulfilling the plethora of legal obligations at the state and federal levels.

Perhaps the most important aspect of a company's incident response plan is their engagement with law enforcement, and the Commission's proposed 4-day disclosure framework could prove detrimental to these agencies' ability to conduct a thorough forensic investigation. The premature and public disclosure of relevant information to the SEC could cause the victim company to accidentally delete or destroy evidence critical to an investigation, as well as jeopardize law enforcement's ability to monitor further malicious activities. Rapid disclosure also decreases the chance of recovering stolen funds, the remediation of cryptographic lockers, or the detection of malicious networks, and the Association believes that it is far more important for restaurants to make appropriate and confidential disclosures to law enforcement than to make premature and uninformative disclosures to shareholders and potential investors.

III. Disclosure Regarding "Material" Cybersecurity Incidents in Periodic Reports

Further complicating this 4-day reporting requirement is how the Commission defines the "materiality" of a cyber incident. Under the proposed rules, an incident would be deemed material if there is a substantial likelihood that a reasonable shareholder would consider this information important in making an investment decision, or if it would have significantly altered the total mix of information available to the investor.[7] Additionally, the Commission's proposed addition of Item 106(d)(2) would require a company to disclosure when a "series of previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate." The SEC says that registrants would be mandated to "analyze related cybersecurity incidents for materiality, both individually and in the aggregate."[8]

Unfortunately, these materiality determinations outlined in the Commission's proposed rules will likely prove challenging for companies to make in a calculated and responsible way, especially while forensic investigations are ongoing, and all the relevant facts have not yet come to light. In fact, many of the examples provided in the proposed rules "are cybersecurity incidents that may happen with frequency in today's cyberthreat environment despite reasonable information security programs and defenses and that could vary in degree of impact from the trivial to the material, depending on the specific facts of the particular incident. The proposed rules do not provide substantially greater clarity from prior guidance for when an incident crosses the materiality threshold."[9] The fact that the trigger date for the disclosure requirement is the same date that the materiality determination must be made does not provide companies with enough flexibility given the rule's expectation that a business should make this determination "as soon as reasonably practicable" after discovery of the incident.

A particularly impractical suggestion in the proposed rule is that disclosure must occur when individually immaterial incidents become material in the aggregate.[10] The SEC made clear that "materiality" would be determined with reference to existing case law, but the Association is unaware of strong, clear case law to reference with respect to aggregate incidents and materiality, and such a requirement would be extremely

[7] SEC Proposed Rules
[8] SEC Proposed Rules
[9] https://datamatters.sidley.com/newly-proposed-sec-cybersecurity-risk-management-rules-and-amendments-for-public-companies
[10] SEC Proposed Rules

difficult to monitor on a continuing basis. Again, realistically, it may take months of diligent work to determine the full scope of any single (or multiple) incident(s) given the complexity, scope, and detailed technical work that must be completed during an incident response. As new material facts come to light during a typical incident response, previous material disclosures will likely need to be revised, updated, and reported (between annual/periodic reports) to correct or update outdated public information. It is not clear how this will benefit shareholders and would most certainly be an undue burden on companies attempting to comply with various laws and regulations in a responsible fashion.

The Association disagrees with the Commission's position that data breaches and security incidents have a material long-term effect on share prices, and we believe the SEC's proposed rules should permit reasonable delays for reporting cyber incidents. A reasonable delay provision would be particularly helpful in circumstances when a company's contractual obligations would require informing a downstream business partner of the notification to the government, but law enforcement deems that informing the affected third party is counter to the investigation's best interests. Further, because of the challenges in assessing or quantifying the impact of a cyber incident during its earliest stages, determining the materiality of one or multiple incidents under the current proposed framework could lead to premature or incorrect disclosures under the 4-day reporting timeline, which would prove more harmful than beneficial to the victim company, law enforcement, and, ultimately, the shareholders themselves. We therefore suggest that the SEC consider including a reasonable delay provision that aligns with the Federal Trade Commission's "without unreasonable delay" reporting standards for personal health information, and ultimately allows for forensics, understanding of damage or impact, and discussion with regulators and plaintiffs to occur while avoiding potential new harms from premature disclosures.

IV. Disclosure of a Registrant's Risk Management, Strategy and Governance Regarding Cybersecurity Risks

The SEC is proposing Item 106(b) of Regulation S-K to require registrants to provide "more consistent and detailed disclosure regarding their cybersecurity risk management and strategy." The Commission argues that disclosure of a company's relevant policies and procedures would benefit investors by improving their understanding of a company's cybersecurity risk profile. Additionally, item 106(c) of the SEC's proposed rules would require disclosure of a company's cybersecurity policies, procedures, and governance strategies, including "the board's oversight of cybersecurity risk and a description of management's role in assessing and managing cybersecurity risks."[11]

While the Association appreciates the Commission's desire to better understand publicly traded companies' cyber incident policies and governance, we believe this aspect of the proposal would create new potential risks for companies by enlightening bad actors to its cyber incident mitigation strategies. The restaurant industry recognizes the importance of establishing cyber risk mitigation policies and are already making great strides in doing so, but the proposal as drafted appears to incentivize specific decision-making processes that may or may not be prudent for a particular organization. Revealing the "secret sauce" behind a company's internal cyber mitigation strategies will only put a bigger target on its back, which ultimately hurts investors by creating more potential for harm to the company than it prevents.

Additionally, pre-existing federal and state data security laws have generally not included a requirement to comprehensively disclose internal policies and procedures unless there is a material weakness in the internal control over financial reporting (ICFR). When this does occur, companies typically disclose the nature of the deficiency leading to the material weakness, their remediation plans, and any changes in ICFR. They are not currently required to provide a detailed description of the controls themselves.

[11] SEC Proposed Rules

The Association suggests that the Commission does not include the disclosure of a company's cybersecurity infrastructure in the final rule unless some kind of confidentiality protection framework is incorporated that would allow companies to demonstrate their preparedness for a potential cyber incident while not creating additional risk exposure for the company and its shareholders.

V. Disclosures Regarding the Board of Directors' Cybersecurity Expertise

Finally, the SEC proposes to amend Item 407 of Regulation S-K by adding paragraph (j) to require disclosure of the cybersecurity expertise of a registrant's members of the board of directors. The Commission's proposed rulemaking says, "[i]f any member of the board has cybersecurity expertise, the registrant would have to disclose the name(s) of any such director(s) and provide such detail as necessary to fully describe the nature of the expertise."[12]

The Association recognizes the importance of firms maintaining robust governance structures and comprehensive compliance programs with a reporting line to escalate cyber issues to senior management and the Board (or Board Committee). We agree with the Commission that Boards should exercise some oversight of cybersecurity programs. However, governance structures are different for companies where cybersecurity is mission-critical (i.e., critical infrastructure entities) compared to companies that merely require good cyber hygiene to operate successfully on a day-to-day basis. Ultimately, the Association believes that the precision of the Board composition reporting requirement to disclose the specific degree of their involvement in approving policies and procedures is hard to quantify, overly prescriptive and difficult to implement in a practical way. Instead, we suggest that it may make sense for the Commission to tailor the Board requirements to CISA-aligned critical industries.

Thank you again for the opportunity to comment on the SEC's proposed rulemaking, "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure." While we support the policy goals behind the proposed reporting, disclosure, and cyber hygiene requirements, the National Restaurant Association urges the Commission to rescind its proposal in its current form due to our concerns about potentially duplicative or conflicting reporting requirements in other federal and state laws, the additional data privacy and security concerns the proposal would inherently create, and its overall effectiveness in better informing company shareholders.

Sincerely,

Brennan Duckett
Director, Technology and Innovation Policy

[12] SEC Proposed Rules