July 17, 2025

Ms. Vanessa Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street NE
Washington, D.C. 20549

Re: Letter in Opposition to the Petition for Rulemaking on the Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Rule (File No. 4-856)

Dear Ms. Countryman,

Consumer Reports, Consumer Federation of America, the Secure Resilient Future Foundation, and the Electronic Privacy Information Center write to oppose any rulemaking to amend the SEC's Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure rule. After only 18 months in effect, disclosure is providing relevant information to investors and helping promote transparency about the security posture of publicly traded firms. This critical information empowers investors to make informed decisions, and enables public- and private sector monitors to track the widespread incidence of cyber attacks.

As for the arguments offered in opposition to Item 1.05, we would like to underscore that the allegations about the impacts of the SEC's requirement are overblown and have no basis in fact.

That has not stopped The American Bankers Association, the Bank Policy Institute, the Securities Industry and Financial Markets Association, the Independent Community Bankers of America, and the Institute of International Bankers from asking for an amendment to the rule that would render it far less effective. They argue that it forces companies to prematurely disclose material cybersecurity incidents and adds costs and complexity to companies' efforts at threat monitoring and cyber incident response. However, we do not think they make a compelling case to repeal Form 8-K Item 1.05 and the corresponding Form 6-K requirements as requested.

The incident disclosure rules went into effect in December of 2023. Item 1.05 required companies that have a cyber incident deemed to have a "material impact" on the company, to disclose that incident via an 8-K no more than four business days after the company has determined that the incident was material. The SEC rule allows companies who are concerned that reporting the incident will adversely impact national security or public safety to seek a delay of between 30 and 120 days from the U.S. Attorney General. There should be nothing controversial as to a public company's timely disclosure of material information related to a cyber-attack, as they would in any other material event.

The SEC provides clarity to combat confusion

In the first six months after the rule took effect, 17 companies filed disclosures under Item 1.05 while 9 filed a disclosure under different rules such as Item 8.01. Based on the disclosures seen, the SEC issued a clarification on May 21, 2024 explaining that companies did not have to file an 8-K under Item 1.05 unless the incident was deemed material.[1]

Under Item 1.05, publicly traded companies that had a cyber incident, but did not yet know if the incident was material, can wait to file until they determined that the incident was material. A later clarification in June 2024 stated that a company could discuss the cyber incident with outsiders such as vendors or consultants hired to help with the incident without running afoul of SEC rules[2].

These clarifications, which opponents characterize as "confusion" surrounding the SEC's new guidelines, are actually evidence of the SEC being responsive to the experiences and needs of affected businesses. Furthermore, the SEC has urged companies to submit filings only for cyber incidents that are likely to have an impact on investors. That ensures that companies don't overburden themselves by reporting breaches that are not material, out of an abundance of caution.

After the May clarification, only 9 companies filed 8-Ks citing Item 1.05, bringing the total filings in the first year to 27. A report published by law firm Debevoise & Plimpton analyzing the change in filings before and after the clarification noted that, "Recent cybersecurity incident disclosures contain more detailed information about affected systems and compromised data, particularly in Item 1.05 filings, than the more general disclosures filed right after the rule became effective."[3]

This history provides a good example of the SEC recognizing that its rules would benefit from refinements to enable them to deliver on their desired goal: greater transparency for investors about the impact of material cyber incidents on publicly traded firms. It also shows that one of the primary arguments made by those seeking to repeal the rules rests on a false premise: that disclosure through Item 1.05 is premature.

The organizations pushing the SEC to repeal Item 1.05 argue that the rule, "has created market confusion and uncertainty as companies struggle to distinguish between mandatory and voluntary disclosures." But recent history casts doubt on that claim. While the market may have

---

[1] U.S. Securities and Exchange Commission "Disclosure of Cybersecurity Incidents Determined To Be Material and Other Cybersecurity Incidents." May 21, 2024. https://www.sec.gov/newsroom/speeches-statements/gerding-cybersecurity-incidents-05212024

[2] U.S. Securities and Exchange Commission "Selective Disclosure of Information Regarding Cybersecurity Incidents." June 20, 2024. https://www.sec.gov/newsroom/whats-new/gerding-cybersecurity-incidents-06202024

[3] Debevoise & Plimpton "Lessons Learned: One Year of Form 8-K Material Cybersecurity Incident Reporting." Feb. 11, 2025. https://www.debevoise.com/-/media/files/insights/publications/2025/02/lessons-learned-one-year-of-form-8k-material.pdf

struggled to comply with the new disclosure law in the immediate aftermath of it going into effect, the SEC's clarifications[4] have largely cleared up that confusion and led to fewer, and higher quality disclosures under the rule. That pattern aligns with corporate and market responses to countless other SEC rules and guidelines over the past 90 years.

Item 1.05 does not chill internal communications

The organizations lobbying the SEC for repeal of Item 1.05 also argue that, "the public disclosure requirement risks chilling candid internal communications and routine information sharing." However, a June 2024 clarification from the SEC makes it clear that such sharing among partners and internal stakeholders should not violate existing SEC regulations (Regulation FD), provided companies understand how Regulation FD governs disclosures. And, given that Regulation FD is two decades old, companies should have that expertise and be able to apply it to a new rule.

Waiting until an incident is mitigated to disclose harms investors and markets

Then there is the argument by opponents that publicly disclosing a cyber incident before it has been mitigated and law enforcement has built a case is "premature." This argument has no factual evidence to back it up, but could empower a breached, publicly traded firm to hide a cyber incident from its investors and the public for years or -perhaps- forever.

Recent history is replete with cases - including the hacks of SolarWinds, Colonial Pipeline or Change Healthcare — in which sophisticated breaches of sensitive firms came to the attention of the public and investors well in advance of the company mitigating the issue or law enforcement completing its investigation of the actors responsible for it. And yet, both internal mitigation efforts and criminal investigations went forward all the same — as they have with the incidents disclosed under Item 1.05 for the past year.

Given that it is common for a cybersecurity incident to take months or even a few years to be mitigated and for law enforcement to build up a case, allowing affected organizations to keep the public in the dark poses a risk to both investors and public health and safety: resulting in operational downtime, lowered sales and even reputational harm. Further, cybersecurity events coming to light via journalism rather than appropriate disclosure may in fact undermine confidence in an affected company's response to a breach. Exposure of material information through public reporting without full and fair information provided by formal disclosure may amplify investor reactions, increase price volatility, and disrupt fair and orderly price discovery in capital markets.

For example, according to a January 2025 report from the Ponemon Institute 58% of organizations hit by ransomware in 2024 were forced to shut down operations in order to

[4] U.S. Securities and Exchange Commission "Disclosure of Cybersecurity Incidents Determined To Be Material and Other Cybersecurity Incidents." May 21, 2024. https://www.sec.gov/newsroom/speeches-statements/gerding-cybersecurity-incidents-05212024

recover. Additionally, 35% of organizations said they experienced brand damage as a consequence of a ransomware attack in 2024[5].

Additionally, IBM's Cost of a Data Breach report noted that the average mean time to contain, or mitigate, a data breach was 258 days[6] and that the cost of the average data breach in the U.S. was $9.36 million Those costs begin accruing once a breach is detected or the malicious actor notifies the company, making it very likely that a significant breach will become material to the firm well before it is mitigated.

As for the arguments that premature disclosure can conflict with national cybersecurity reporting requirements or harm law enforcement efforts, the Ponemon ransomware study indicates that only 28% of companies experiencing a ransomware attack called law enforcement[7]. So, not only does the existing rule already provide a mechanism for delaying reporting when national security or legal investigations require it, in the majority of cases, companies experiencing incidents do not call on law enforcement for help.

Hackers using SEC disclosure to extort investors ignores the real threat

It's clear that cyber incidents can have a material impact on a company's finances, operations or reputation, so waiting to disclose these incidents can harm investors and markets. But does forcing a company to report a cyber incident to the SEC in a public filing also harm the reporting company? The financial entities seeking repeal argue that it does, because they say such disclosure has been weaponized by hackers as an extortion method.

We find this logic questionable. When malicious hackers find a vulnerability and exploit it, if the incident is inconsequential, and thus immaterial, then the company would not need to report it and the attacker has no leverage with which to extort the company. If the attack is material, the threat of disclosure when disclosure is already required removes the potential for extortion. Absent Item 1.05 one could see hackers attempt to extort a company on the basis that they have caused a material incident that leads to financial losses or large ransomware payments that might need to be disclosed under other rules.

Additionally the threat of disclosure through the SEC is an inefficient threat. Any hacker seeking to extort a company for money can elect to use ransomware or the threat of data loss to encourage payment. In reality, the damage — from the perspective of investors and public health and safety — is that the hacker has found a way into the company's IT environment and

---

[5] The Global Cost of Ransomware Study. Conducted by Ponemon Institute for Illumio. Published January 2025. https://cdn.prod.website-files.com/63e25fb5e66132e6387676dc/67991cfb5c7890992f292383_The-Global-Cost-of-Ransomware-Study.pdf

[6] Cost of a Data Breach Report 2024. Conducted by Ponemon Institute on behalf of IBM. Released June 30, 2024. https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec.

[7] The Global Cost of Ransomware Study. Conducted by Ponemon Institute for Illumio. Published January 2025. https://cdn.prod.website-files.com/63e25fb5e66132e6387676dc/67991cfb5c7890992f292383_The-Global-Cost-of-Ransomware-Study.pdf

has access to its data, the ability to disrupt operations, or both. It is not that they can damage the firm's standing with the SEC and public markets. Suggesting that the SEC bow to the tactics of ransomware groups by pulling back a rule designed to promote private sector transparency and accountability is wrong-headed.

Liability isn't the harm — hacking is the harm

The same logic can also be applied to the argument that premature disclosure to the public markets can cause harm through increasing liability or changing the cost of insurance for the affected companies. Here disclosure is not the problem. Rather, it is the ability of cybercriminal and state sponsored attackers to readily hack the company. The response the company has to the hack will determine its insurance costs, payouts and the potential liability. As of February 13, 2025, Kane McGladrey, a CISO in residence at Hyperproof, wrote that there had not yet been a lawsuit filed as a result of the SEC's public disclosure rules[8].

Businesses are still behind when it comes to boosting their overall security and resilience in the face of a rapidly escalating cyber threat environment. For example, a study by Ponemon Institute that interviewed 650 IT professionals noted that only 46% had an incident response plan that was applied consistently across the organization and 28% had no plan or an ad hoc plan. An incident response plan is an essential tool for managing any sort of cyber incident[9]. Requiring companies to disclose their incidents relatively quickly after determining their materiality is a useful impetus to drive companies to adopt incident response plans in advance.

Cisco also tracks cyber readiness through an annual index that shows only 4% of companies are mature when it comes to their cyberreadiness which is up from 3% the year prior. The index also indicated that only 34% feel very confident in the resilience of their organization's current cybersecurity infrastructure against attacks.

Public disclosure of cyber incidents has an investor and public benefit

Finally, in response to the escalating threat environment we find that public disclosure is a helpful and possibly preventative measure to help companies build the resilience and cyber readiness that they need. Public disclosure of attacks can help identify when threat actors target specific sectors, allowing investors, competitors, and law enforcement to see that a popular Russian cyber criminal gang may be attacking retail stores or the airline sector.

They can also help identify weaknesses in third-party software or partners that might be shared across different reporting companies. Verizon's 2025 Data Breach Investigations Report noted

---

[8] Kane McGadrey. "Results from the First Year of Cybersecurity Incident Filings on Form 8-K." LinkedIn. Feb. 13, 2025.
https://www.linkedin.com/pulse/results-from-first-year-cybersecurity-incident-form-8-k-mcgladrey-fttuc/

[9] 2024 Cybersecurity Threat and Risk Management Report. Conducted by Ponemon Institute on behalf of Optiv. Published June 2024.
https://www.optiv.com/insights/discover/downloads/2024-cybersecurity-threat-and-risk-management-report

that in 30% of the breaches investigated, there was some form of third party involvement, up from 15% the year prior.[10]

In conclusion, the rules requiring companies to respond quickly to cyber incidents; determine if those incidents are likely to have a material impact on shareholders' decisionmaking; and then disclose those incidents publicly are beneficial to investors, national security, and public health and safety. The arguments made by those wishing to repeal this rule seek to hide a lack of cyber readiness behind flimsy claims that have been addressed by clarifications in the rules and have so far have failed to come to fruition. We recommend that the SEC keeps Item 1.05 as part of the Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Rule and focuses on enforcing the rule.

Thank you for your attention to this matter, and if you have any questions, please contact me at stacey.higginbotham.consultant@consumer.org.

Sincerely,

Stacey Higginbotham
Policy Fellow
Consumer Reports

Paul F. Roberts, President
Secure Resilient Future Foundation Inc.
paul@secure-resilient.org

Susan Weinstock
Chief Executive Officer
Consumer Federation of America

Electronic Privacy Information Center

[10] Verizon 2025 Data Breach Investigations Report. Published April 23, 2025. https://www.verizon.com/business/resources/Taca/reports/2025-dbir-data-breach-investigations-report.pdf