TransUnion

May 9, 2022

Securities and Exchange Commission
100 F Street NE
Washington DC, 20549

Re: File Number S7-09-22 SEC's Proposed Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

To Whom It May Concern:

TransUnion welcomes the opportunity to comment on the Security and Exchange Commission's proposed rule. As one of the three nationwide credit reporting agencies (CRAs), we hold valuable data that enables businesses, customers, and consumers to transact with confidence. We are committed to protecting that information and ensuring that our regulators, investors, consumers, and associates have adequate and useful information about our operations, including responsible disclosure of cyber risks and incidents. To ensure that we remain vigilant stewards of data, we act with care and responsibility with the data we source, analyze and protect, leveraging advanced technology and an uncompromising stance toward information security, ethics and governance. With a strong emphasis on these frameworks and highly qualified associates, we safely provide data solutions that help consumers, businesses and the economy.

This letter provides our perspectives on:

I. Materiality
II. Ongoing Investigations
III. Timing of Notifications
IV. Potential for Additional Risks

I. Materiality

The proposed rule relies on the concept of materiality as a trigger for required reporting. While the rule appropriately allows time for a firm to determine whether an incident is material, the lack of definition for what constitutes a "material" breach leaves companies subject to the rule without clarity as to the key determination that must be made. Although the concept of materiality has been applied to disclosures of other sorts, those situations have the benefit of decades of case law, guidance, and analysis to direct the determination. The standard for what constitutes a cyber issue of significance to a reasonable investor is far less clear, and – without more – will likely remain a moving target, subject to refinement in litigation.[1] Furthermore, this lack of clarity will likely prove an inviting target for frivolous lawsuits that will distract the attention

[1] The examples set forth in Section B.2 highlight this challenge. What the threshold would be for an investor to be concerned about one of these types of incidents is very difficult to predict. And over-disclosure, as the materiality standard implicitly recognizes, is far from costless – in the current environment, it would likely involve substantial amounts of unnecessary work reporting the range of incidents that a company may face.

of a firm's information security experts from performing their most important duties. To address these issues, any final rule must include greater definition to ground the principle of materiality in more objective and readily applicable parameters.

The term "material in the aggregate" poses similar issues. More definition is needed as to how a company should aggregate – Which incidents are sufficiently related? How many incidents constitute "material in the aggregate"? Additional information is needed to ensure that companies can effectively and efficiently comply with the law.

II. Ongoing Investigations

Investigations into potential cybersecurity incidents are highly sensitive matters where extreme caution is required to avoid alerting a potential bad actor about what the company knows and what it is planning to do. Early disclosure can alert the source of a threat, undermining the ability of a company to identify and remediate issues and inhibiting the determination by a company or law enforcement of the identities of bad actors and their methods. The proposed rule's preemption of a notification delay for internal and external investigations, even in the face of a law enforcement request, runs contrary to these essential functions, and to the expressed view of other government agencies requesting notification holds.[2] The interest of investors in transparency cannot override the need to effectively resolve an issue and prevent its reoccurrence, which itself is in the interest of not just one company's shareholders but the shareholders of any other company that may be under a similar threat. Any final rule should incorporate a notification delay (or at least a delay of public notice) to allow companies and government agencies the ability to complete their investigation uninhibited.[3]

Relatedly, while we appreciate the motivation behind disclosing more information to investors, the rule fails to explain why investors need reporting of an ongoing investigation – with all the uncertainty and lack of firm conclusions that entails – rather than a final report that provides complete and well-vetted analysis of an incident and its impact. Unless there is a particular reason for early notification to investors, the Commission need not apply the same timeline to investor notification as it does to Commission notification, and should instead require the filing of the Form 8-K only after a final report can be issued.

III. Timing of Notifications

The proposed rule sets a deadline of four business days from the determination of materiality to the filing of the Form 8-K. That turnaround is simply too short to collect and present the necessary information accurately and will inevitably lead to mistakes that do the opposite of what the rule intends – disclosures will misdirect the Commission and investors, rather than provide clarity.[4] Furthermore, as noted above, a notification at such an early stage – even of the limited set of information requested by the Commission – could be detrimental to the ongoing investigation and remediation. Accordingly, a final rule must allow for more time from the determination of materiality to the disclosure.

[2] Many jurisdictions, including the federal government under HIPPA, explicitly recognize the necessity of delayed no ification where law enforcement makes such a request.

[3] The proposal asks whether a notification delay should be permitted where the Attorney General makes a written determination that the delay would be in the interest of national security. While this would be a good step, it is far from sufficient, as it doesn't allow for other law enforcement agencies or companies to express similar pressing needs.

[4] The proposed rule does not set forth any specific reason why four days, rather than a somewhat longer period of time, is appropriate.

IV. Potential for Additional Risks

Finally, before finalizing any rule relating to the disclosure of cybersecurity incidents, policies, procedures, and governance, the Commission should solicit and review specific comments relating to whether this type of information may actually assist threat actors in identifying potential targets. Even a cautious firm may – in endeavoring to be responsive to the Commission's directives – inadvertently reveal a detail that would provide a window into the firm's security protocols. Without fully analyzing this risk and ensuring that the rules will set forth parameters and limits to ensure that this does not happen, the potential for negative unintended consequences will remain high.

In conclusion, we appreciate the Commission's willingness to examine and develop best practices around cybersecurity incidents. TransUnion looks forward to working with the Commission in its effort to enhance and standardize disclosures related cybersecurity risk management. If you have any questions, please reach out to Allison Shuster, Head of U.S. Government Relations, at [redacted].

Sincerely,

Bill Shields

Executive Vice President, Information Security
TransUnion