

Mark J. Guinan
Executive Vice President and Chief Financial Officer



May 9, 2022

Via Electronic Mail (rule-comments@sec.gov)

U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090

Attention: Ms. Vanessa Countryman, Secretary

Re: File No. S7-09-22
Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure
Release Nos. 33-11038; 34-94382; IC-34529

Dear Ms. Countryman:

Quest Diagnostics Incorporated (“Quest Diagnostics”) appreciates the opportunity to submit to the U.S. Securities and Exchange Commission (the “Commission”) its views on the rules proposed in the above-captioned release in respect of disclosures regarding cybersecurity risk management, strategy, governance, and cybersecurity incident reporting (the “Proposed Rules”).

Quest Diagnostics is the world’s leading provider of diagnostic information services. Our diagnostic information services business provides information and insights based on our industry-leading menu of routine, non-routine and advanced clinical testing and anatomic pathology testing, and other diagnostic information services. Our diagnostic solutions businesses are the leading provider of risk assessment services for the life insurance industry and offer healthcare organizations and clinicians robust information technology solutions.

We appreciate the Commission’s attention to the increasing risks to public companies posed by cybersecurity threats and its efforts to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance and cybersecurity incident reporting to better inform investors. While we support certain of the amendments included in the Proposed Rules, we have concerns regarding the cybersecurity incident reporting requirements as formulated under the Proposed Rules.

In particular, we believe the cybersecurity incident reporting requirements, as proposed, will serve only to benefit parties other than investors. The scope and timing of the proposed

incident reporting could potentially force companies to prematurely disclose incomplete information, which would confuse investors and negatively impact a company's stock price with hastily disclosed information. The rush to disclose information that is evident in the Proposed Rules would likely end up interfering with the ability of companies to respond to ongoing cybersecurity incidents, including hindering remediation efforts. Importantly, the primary benefactor of the information that would be disclosed in connection with the proposed incident reporting requirements may be the bad actors that are initiating these attacks and even the bad actor who initiated the very attack that is subject of the premature disclosure.

Specifically, we believe that imposing an affirmative obligation to report material cybersecurity incidents on Form 8-K within four business days of a materiality determination would result in premature disclosure that would hinder the ability of public companies to stop, investigate, remediate and defend against cybersecurity incidents. While we recognize that cybersecurity events can be material and investors should be appropriately informed of instances of these types of events, we do not think a material cybersecurity event should trigger an immediate disclosure obligation. Although Form 8-K has identified certain events that trigger current reporting, Form 8-K is not designed to encompass all material events that a company could experience. For example, there is no Form 8-K triggering event if a company determines that its financial results for a period will not meet its publicly disclosed financial guidance. There could be many instances where the disclosure of a small "miss" on stated guidance would have an immediate stock price impact that would be far greater than any disclosure related to the occurrence of a material cybersecurity event. The securities laws do not impose an affirmative duty to disclose material information on a current basis and the Proposed Rules are not directed at updating information that was misleading when it was initially disclosed. The Proposed Rules are seeking to impose unique treatment for a specific type of information without consideration of the challenges and pressures a company faces in preparing these types of disclosures and the ability of investors and the market to absorb the information delivered prematurely.

Accordingly, we are recommending that the Commission should not adopt proposed new Item 1.05 of Form 8-K. If the Commission determines that it is important to require an affirmative obligation for public companies to report material cybersecurity incidents, we suggest that, as an alternative, the Commission adopt a different incident reporting disclosure regime, which we believe would allow companies to provide more accurate, comprehensive and actionable disclosures to investors about material cybersecurity incidents, while preserving the Commission's goal of having public companies provide investors with consistent cybersecurity incident disclosures that are comparable across industries.

Outlined below are our comments on the Proposed Rules.

Proposed Item 1.05 of Form 8-K

The Proposed Rules mandate, under a new Item 1.05 of Form 8-K, certain cybersecurity incident disclosures within four business days after a registrant determines that an incident is material, which materiality determination must be made "as soon as reasonably practicable after discovery of the incident" in accordance with Instruction 1 to Item 1.05. In particular, a registrant would be required to disclose the following information about a material cybersecurity incident

to the extent known at the time of filing: when the incident was discovered and whether it is ongoing; a brief description of the nature and scope of the incident; whether any data was stolen, altered, accessed or used for any other unauthorized purpose; the effect of the incident on the registrant's operations; and whether the registrant has remediated or is currently remediating the incident. Material changes, additions or updates in the relevant period, if any, to information previously disclosed under new Item 1.05 of Form 8-K would be required to be included in a company's quarterly reports on Form 10-Q and annual reports on Form 10-K, as applicable, and potentially even in an amended Form 8-K.

Interference with Ability to Investigate Cybersecurity Incident

Investigating the nature, impact and costs of cybersecurity incidents can often be a highly complex, specialized and time-consuming process, particularly given the increasing frequency and the rapidly evolving sophistication and intensity of cyberattacks in recent years. We believe that, in many instances, under the Proposed Rules, a company would have insufficient time to gather enough information to determine whether a known cybersecurity event is material. Moreover, even if a company believes that a cybersecurity event is material, four business days is insufficient for companies to conduct the necessary investigations to collect the information required by Item 1.05, particularly given the need to engage with internal and external experts. This timeframe seeks to rush out disclosures related to cybersecurity matters without taking into account the circumstances surrounding, and the magnitude and complexity of, any given cybersecurity incident. Under proposed Item 1.05, we believe companies will be under intense pressure to quickly make a determination regarding whether a known cybersecurity event is material.

Instruction 1 to proposed Item 1.05 reinforces the pressure that this new obligation will place on companies by requiring "a registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident." As a result, it is likely that a company will feel compelled, within a four business day window, to either hastily conclude that a known cybersecurity event is material or disclose the existence of a cybersecurity event, even if it does not know whether it is material, for fear of being second-guessed when more information becomes available. Stockholders, regulators and plaintiff's law firms, with the benefit of time, less pressure and the full landscape of information and impact, may seek to challenge the determinations made by management in the heat of an ongoing cybersecurity event where the information is incomplete and unverified. These parties will ask the simple question, informed by hindsight: "How could you not think it was not material?"

The proposed reporting regime will cause companies to make disclosures related to cybersecurity events that are incomplete. To meet the proposed four business day deadline, companies will likely make disclosures that are required by proposed Item 1.05 and indicate that the company has not been able to conclude whether the cybersecurity event is material. As a result, a Form 8-K filing, at this stage, will do more to confuse investors than to inform them. The market reaction to a premature disclosure of a cybersecurity event could be significant. The

lack of clarity and the absence of a clear assessment on materiality in a Form 8-K filing will lead to speculation.

Interference with Company Response and Law Enforcement

Furthermore, as the Proposed Rules do not distinguish between ongoing and past cybersecurity incidents, in the case of an active incident, a premature filing of a Form 8-K could provide a malicious actor with valuable intelligence on the current vulnerabilities in the company's systems and the company's ability to defend against a cyberattack, and as a result exacerbate the severity of the incident or hinder its remediation. For example, in the case of a ransomware attack, the ability to negotiate and thwart an attacker could be compromised by a premature disclosure of the existence of the attack. Disclosure should not be required at a time when a company believes that disclosure would interfere with its response to an incident.

We are also concerned with the proposed sequencing of the cybersecurity incident reporting requirement. The Proposed Rules provide that companies would be required to first file a Form 8-K reporting the material cybersecurity incident pursuant to Item 1.05 of Form 8-K and to subsequently update such information on a quarterly basis in a company's Form 10-Q and Form 10-K, as applicable, pursuant to Item 106(d). The Commission has also indicated that, notwithstanding Item 106(d), there may be situations that would require amending the Form 8-K reporting the material cybersecurity incident as a result of subsequent developments regarding the incident. As described above, information regarding cybersecurity incidents often becomes available to companies incrementally and incompletely. Requiring that a company determine whether an amendment is required as a result of a subsequent development would subject the company to the same struggle of assessing when this disclosure should be made and what it should include while avoiding further investor confusion.

In addition, we are also concerned that proposed Item 1.05 does not permit disclosure to be delayed when law enforcement determines that public disclosure would impede a civil or criminal investigation. As the Commission notes in its release, certain jurisdictions have laws that allow companies to delay providing public notice about a data breach incident or notifying certain constituencies of such an incident if law enforcement determines that notification will impede a civil or criminal investigation. By implementing Item 1.05 of Form 8-K, disclosures may be required on Form 8-K even where disclosure would hinder an active civil or criminal investigation on the basis that such disclosures are "critical to investor protection and well-functioning, orderly, and efficient markets." We disagree with this premise and do not believe Form 8-K should impose an affirmative reporting obligation where disclosure would hinder law enforcement in its investigation and identification of the actors behind a particular incident, not least because doing so would do nothing to prevent future cybersecurity incidents and may even make them more likely.

As described above, we appreciate the Commission's attention to the increasing risks posed by cybersecurity threats and acknowledge that information about such threats may be relevant to investors and other market participants by enabling them to assess the potential effect of a material cybersecurity incident on a particular registrant. We believe that the existing reporting regime sufficiently facilitates such disclosures—companies already choose to report cybersecurity incidents under Item 8.01 of Form 8-K and may do so without the imposition of

time constraints that could result in incomplete disclosure or impede responding to the incident or law enforcement investigations. While the existing regime does not impose an affirmative obligation to report a material cybersecurity incident, neither does it impose an affirmative obligation on a company to disclose a whole range of information that is material. The foundation of the existing reporting regime does not allow a company to omit material information when communicating with the market, which we believe maintains the investor protection and market efficiency that the Commission seeks.

Because of the complexity of cybersecurity incidents and negative consequences of premature reporting thereof, we do not believe an affirmative obligation to report material cybersecurity incidents on Form 8-K within four business days is appropriate, and we believe that the Commission should not adopt proposed new Item 1.05 of Form 8-K.

Alternative Proposal for Cybersecurity Disclosures

If the Commission determines that it is important to require an affirmative obligation for public companies to report material cybersecurity incidents, we suggest that, as an alternative to the new Item 1.05 to Form 8-K, the Commission propose modifying the new Item 106(d) applicable to quarterly reports on Form 10-Q and annual reports on Form 10-K to include the Item 1.05 disclosures, rather than implementing new Item 106(d) only for purposes of updated incident disclosure as contemplated under the Proposed Rules. Under this alternative proposal, registrants would be required to disclose, to the extent known at the time of filing, information with respect to any material cybersecurity incidents that took place during the period covered by the quarterly or annual report, as applicable, and provide material changes, additions or updates in the relevant period, if any, to previous material cybersecurity incident disclosures as currently set forth in Item 106(d). To the extent available, companies would also be able, but not required, to disclose information regarding material cybersecurity incidents that occurred between the end of the reporting period and the date of filing of the Form 10-K or Form 10-Q, as applicable.

Under this approach, Item 106(d) should be modified also so that a company would be permitted to delay reporting to the next quarterly or annual report, as applicable, to avoid interference with a company's response to the incident or law enforcement investigation. Despite this exemption, companies would continue to be able to use Form 8-K or periodic reports to report information regarding cybersecurity incidents under appropriate circumstances.

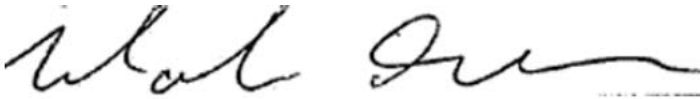
We note that this suggested approach is consistent with legal proceedings disclosures under Item 103, which are required, if applicable, on a quarterly basis in quarterly and annual reports. Assessing materiality and gathering relevant information with respect to pending legal proceedings can often be time consuming, and premature disclosure of such proceedings may hinder, rather than aid, investors in understanding the proceedings. Similar to Item 103, under the suggested approach, companies would be required to provide material updates in the relevant period to a previously disclosed material cybersecurity incident to inform investors of incident developments as facts evolve.

We believe such an alternative will provide companies more time to investigate cybersecurity incidents and uncover information regarding material cybersecurity incidents, thereby allowing companies to evaluate and assess their nature, scope, and impact on financial

conditions and operations in a more comprehensive manner. We believe that the suggested alternative also would reduce the negative consequences, outlined above, of mandating reporting on Form 8-K. While we acknowledge, as the Commission notes, that this would lead to less timely reporting on material cybersecurity incidents on the whole, we believe the benefits of this approach, which include more complete disclosures, decreased likelihood of malicious actors exploiting vulnerabilities resulting from the material cybersecurity incident and interference with a civil or criminal investigation and reduced compliance costs for companies, far outweigh this consideration and will allow for disclosures that are more useful to investors and other market participants and more digestible by the markets. We also believe this proposal provides a uniform standard of disclosure so investors and other stakeholders will be able to locate and compare disclosures across all public companies in a consistent manner.

We appreciate the opportunity to express our views and concerns regarding the Proposed Rules. If there are questions regarding any of our comments, we would welcome an opportunity for further discussion. Please do not hesitate to contact me at 973-520-2700.

Sincerely,

A handwritten signature in black ink, appearing to read "Mark J. Guinan". The signature is fluid and cursive, with a long horizontal stroke at the end.

Mark J. Guinan
Executive Vice President and Chief Financial Officer

cc: Michael E. Prevoznik, Senior Vice President and General Counsel
William J. O'Shaughnessy, Jr., Deputy General Counsel and Corporate Secretary