GRANT THORNTON LLP
Grant Thornton Tower
171 N. Clark Street, Suite 200
Chicago, IL 60601-3370

D +1 312 856 0200
S linkd.in/grantthorntonus
twitter.com/grantthorntonus

June 7, 2024

Office of the Secretary
Public Company Accounting Oversight Board
1666 K Street NW
Washington, DC 20006-2803

Via Email to comments@pcaobus.org

Re: PCAOB Rulemaking Docket Matter No. 055, *Firm Reporting*

Dear Office of the Secretary:

Grant Thornton LLP appreciates the opportunity to comment on the Public Company Accounting Oversight Board's (PCAOB's or Board's) Rulemaking Docket Matter No. 055, *Firm Reporting*. We respectfully submit our comments and recommendations for the Board's consideration.

The Board indicates that the changes discussed in the Proposal are "necessary or appropriate in the public interest or for the protection of investors and, if adopted, would enhance firm transparency and improve PCAOB oversight of firms."[1] We believe that responsible and appropriate transparency can enhance stakeholders' understanding of individual audit firms. However, we are concerned that the Board's basis for the nature and breadth of the proposed transparency requirements remains unclear, as many direct benefits of implementing the proposed requirements are presented with caveats indicating known and suspected limitations to their usefulness. We question whether certain proposed reporting requirements would be useful and whether the proposed enhanced reporting would be meaningful to investors. We also question the cohesion of certain of the proposed reporting requirements with other standard-setting and rulemaking projects and note that this Proposal could result in the unnecessary duplication of firms' efforts in reporting information to the PCAOB. These concerns, along with practical application challenges, indicate a troubling imbalance between avoidable cost challenges and the perceived potential benefits of firm reporting.

[1] Page 4 of PCAOB Release No. 2024-003 (the Proposal).

Proposed changes to Form 2

Fee information

In considering the Proposal, we have several concerns related to the proposed enhanced fee information reporting requirements affecting Form 2. The potential value to the Board and to other stakeholders of further disaggregating fees for audit services is unclear, particularly when the proposed reporting includes entities that are not subject to the oversight of the PCAOB. We believe that such information in Form 2 could be misleading to outside stakeholders who may mistakenly believe that such services related to fees are within the PCAOB's purview, when in fact the disclosures include fees from services provided to entities that are not issuers or broker-dealers and therefore are not within the PCAOB's purview. This is in direct contradiction to the clarification and distinction between services subject to and not subject to PCAOB oversight that the Board is attempting to make in their proposed Rule 2400, *Proposals Regarding False or Misleading Statements Concerning PCAOB Registration and Oversight and Constructive Requests to Withdraw from Registration*.

Additionally, it is unclear what the term "all clients" means, as shown in Item 3.2(a) within the appendix to the Proposal. We believe the ambiguity could create inconsistencies in calculations since some firms may interpret it to mean all clients of the firm, while others may think it means all clients of the audit practice.

The proxy fee categories in the Proposal correlate to those currently used by SEC issuers for their proxy reporting. Firms report fees by these proxy fee categories in Form 2, and the fees are based on information disclosed publicly by SEC issuers for their proxy reporting. Therefore, stakeholders could currently reconcile fee disclosures between a registered firm and their issuer clients. Conversely, further disaggregation of fees included in the Proposal, which is currently not maintained or reported by firms, could not be reconciled to publicly reported proxy fee information, particularly for private company clients this inclusion of which would be required. We do not believe this will be helpful to investors.

Should the PCAOB choose to keep the disclosures regarding nonissuer fees, we believe it should not be reported using SEC fee categories that a private company is not required to comply with. However, we strongly urge the Board to eliminate the proposed breakdown of fees for other services rendered for the reasons described above.

Additionally, we believe that the proposed change to present total fees in actual dollar amounts would not be meaningful to stakeholders and that the more meaningful measure of fees per issuer is already provided to investors in SEC filings. Although the intention of the Board with this aspect of the Proposal is to decrease inconsistency among current reporting on Form 2, we believe presenting fees in dollars would, in fact, detract from comparability among audit firms, given the vast difference in the size of firms serving as issuer and broker-dealer auditors. Such reporting would also shift the focus away from the size of a firm's issuer audit practice to the size of its practice as a whole, which may not be useful to investors or audit committees.

If the Board proceeds with the proposed fee reporting changes, we believe the Board would need to institute some level of materiality or de minimus threshold for the proposed fee information. Under the current Form 2 reporting requirements, it would take a material difference in fees to shift the percentage that is reported. Alternatively, if actual dollars are included as proposed with no materiality thresholds provided, a single dollar error in a reported amount would trigger the need to file an amended Form 2. If the Board seeks to truly inform stakeholders and investors about firms' fees, we believe it is important to recognize that de minimus differences likely will not impact transparency for stakeholders.

In order to retain the usefulness of the information provided and to avoid potential confusion, we recommend maintaining the extant requirement to report issuer audit and nonaudit services as a percentage of total firm revenue for the reporting period. We believe removing the additional proposed disaggregation would allow stakeholders to remain focused on meaningful metrics when it comes to considering a firm's audit practice mix.

However, if the Board does proceed with the proposed dollar fee disclosure, we strongly suggest that the disclosure require only fees billed to issuer audit clients that would match the fees paid to their independent auditor already disclosed by issuers in SEC filings.

Firm financial statements

We agree that financial statements provide stakeholders with a comprehensive view of a company's performance and financial health. However, the goal of the proposed requirement is different from the intended purpose of an entity's financial statements. The proposed requirement is intended to enhance the Board's oversight and monitoring of the health of large registered public accounting firms in order to identify potential solvency issues or a lack of resources to deliver quality audits. But it is unclear from the Proposal what the Board will do when its monitoring identifies these issues. As the Proposal does not currently specify how the PCAOB will act upon having this financial information, including indicators of financial distress, we are concerned that the Board has not demonstrated why the proposed requirement is in the public's best interest or why the PCAOB has an administrative need for this information. Further, the PCAOB already has access to accounting firms' performance and financial information through its inspections process.

In addition, we are concerned with the proposed requirement for firms to submit to the Board financial statements in accordance with the applicable financial reporting framework of the firm's jurisdiction, such as accounting principles generally accepted in the United States of America (US GAAP). We do not believe it is reasonable or appropriate for registered public accounting firms to be required to prepare US GAAP financial statements when this may not be the most meaningful framework for their business or operations. What's more, we do not foresee the Proposal's perceived benefits for stakeholders outweighing the cost and resources needed to convert firms' financial statements, including disclosures, to the applicable financial reporting framework of the firm's jurisdiction.

If the Board moves forward with this requirement, we emphasize the importance of maintaining the confidentiality of a firm's financial statements, both upon initial submission and indefinitely after they are submitted. If firms' financial statements were publicly reported, there could be unintended operational or financial consequences, as well as impacts to healthy competition within the industry. We believe that disclosing firms' financial statements publicly could result in misleading outside stakeholders to believe that all information therein, even information related to other (private) companies under audit and other service lines, lies within the PCAOB's purview. Should the Board intend to make accounting firms' financial information public after further analysis, we believe any changes to confidentiality should be subject to the PCAOB's due process, including the opportunity for public comment.

Governance

We agree with the Board that audit quality is linked to strong firm leadership and governance. Nevertheless, we noted a few instances of duplication within the Proposal, as well as instances of duplication or inconsistency with the recently approved QC 1000, *A Firm's System of Quality Control*. We believe such instances require resolution in a manner that is efficient for and clear to accounting firms. For example, QC 1000 requires governance information to be reported confidentially, while the same information in the proposed requirements would be made public. If the Board proceeds with the proposed governance reporting requirements, we believe the information should be reported only once and it should be reported to the PCAOB confidentially under QC 1000.

Network information

We agree with the Board's observation that network arrangements provide a variety of benefits to its members. The Board notes in the Proposal that it currently receives information regarding member firms within a network.[2] However, generally, a network organization itself is not registered with the PCAOB, and, therefore, the PCAOB does not have statutory oversight over those networks. We do not believe it is appropriate for the PCAOB to extend its requirements to compel member firms to submit network-specific information to the PCAOB. We are concerned that requiring member firms to make disclosures about the network puts the member firms in a challenging position with the network. It is possible that confidentiality agreements between the network organization and member firms exist that preclude the member firm from publicly disclosing information related to the network. Additionally, an individual member firm may not be privy to all network information that the PCAOB proposes to obtain. Because the network itself is not within the PCAOB's jurisdiction, we believe the related disclosure requirements should be eliminated in the final rule.

Cybersecurity policies and procedures

While we agree with the PCAOB's observation that cybersecurity incidents have increased in recent years in size, frequency, and sophistication, we believe the proposed requirement related to cybersecurity policies and procedures is unclear. We are concerned that disclosure of how firms manage cybersecurity risks may provide

[2] Page 33 of the Proposal.

data points to cyber-criminals to assist them in breaching a firm's defenses. We believe it is appropriate to require firms to report that they have certain policies or procedures in place, but disclosing details or contents of cybersecurity policies and procedures seems to create (instead of inhibiting) opportunities for bad actors to be successful. Further, the PCAOB already has access to firms' cybersecurity policies in the course of its inspections and regularly interviews cybersecurity personnel to learn more about their internal programs and procedures.

It must also be emphasized that clients of public accounting firms are very capable of doing their own due diligence on their service providers. Public accounting firms serve corporate clients with sophisticated procurement procedures, and clients have an opportunity to vet the cybersecurity policies of the firm they choose to engage. These corporate clients regularly conduct due diligence on their service providers during the RFP process and throughout the relationship. Clients of all sizes and industries regularly ask for extensive information on firms' cybersecurity programs and policies, and they protect their interests through contract terms. In our opinion, the PCAOB's role as an intermediary between a firm and its clients is not necessary and reaches beyond the bounds of the PCAOB's jurisdiction.

Proposed changes to Form 3

We believe the proposed accelerated deadline could present significant challenges with regard to compliance. The Board points to automation and enhancements of technology as a reason for the shorter deadline; however, the nature of events that would fall under Form 3 reporting are not conducive to automation. Therefore, we believe the basis for the accelerated deadline is inconsistent and seemingly irrelevant to the details of the proposed changes to Form 3. In addition, we have seen no evidence to suggest that there is any need or benefit to investors of shortening the time period. Conversely, we believe that 14 days provides very little leeway for firms to provide the information and would entail unnecessary costs. This is particularly the case given the increased reporting requirements set forth in the proposed rule. We are concerned that the shortened requirement may disproportionately impact non-US firms because there may be legitimate issues as to whether a matter should be reported, whether a matter should be confidential, and/or whether a firm should withhold information due to legal conflicts. We encourage the Board to reconsider the accelerated deadline in light of the types of events that would be subject to Form 3 reporting.

We also believe the proposed requirement is overly broad and subject to hindsight bias. Current requirements include discrete events that can be reasonably monitored. By expanding the list to include an ambiguous set of possible scenarios, the Board may be creating operational challenges in maintaining sufficient quality management controls over the completeness of Form 3 reporting.

Proposed cybersecurity incident reporting

We have considerable concerns with the appropriateness and operationality of the proposed reporting around cybersecurity incidents.

We do not believe the proposed requirement is sufficiently clear. In particular, it is unclear what is scoped into the term *"*critical operations*"* as used in the proposed requirement. There are many internal systems that are critical to a firm's success or growth and may even be essential for a firm to manage its business overall, but a temporary disruption of such systems should not necessarily warrant a reportable event. For example, would disruptions or degradations of a temporary nature to a firm's performance management system, or to its website or budgeting software, become reportable events to the PCAOB even if they do not impact audit quality or the ability to continue serving audit clients, nor compromise any client data?

The proposed rule seems to emphasize the urgency of reporting an incident to the PCAOB, as opposed to fostering the resolution of the incident to mitigate potential risks to the firm and clients and to prevent the disruption of services to clients. The underlying purpose for urgently reporting these incidents to the PCAOB is unclear, as well as what steps the PCAOB intends to take once notified. When resolving an incident, time is of the essence in order to investigate, contain, and remediate the risks. The PCAOB does not have a role in that process, nor the means to assist firms in ensuring a better resolution. Indeed, responding to inquiries from the PCAOB in the midst of a crisis could instead divert efforts and attention away from remediating the incident itself (see additional comments below).

Further, while the PCAOB suggests that reporting incidents that seem reasonably likely to manifest in future harm could assist other firms in mitigating their risks, there is no reference in the proposal as to how that would occur. And, the required reporting of disruptions that do not impact audit quality, the ability to continue serving audit clients, nor involve a compromise of proprietary client information (limited to audit clients), does not seem to have a clear connection to the PCAOB's stated goals or objectives.

An alternative approach would be to bifurcate reporting: (i) mandatory confidential reporting for incidents that have actually occurred and that could impact the firm's ability to continue serving audit clients or audit quality or could compromise audit client information, and (ii) a voluntary reporting system for other types of incidents. The PCAOB may also consider how it could assist firms by issuing alerts or bulletins to other firms as to incidents that are voluntarily reported. The awareness could help firms manage their threat environment and risk profile, even though tools for such threat monitoring are already commercially available.

Confidentiality

We believe cybersecurity incident reporting should be kept completely confidential, especially if the final rule will require incident reporting within a few days of occurrence, during which time, the impact is still being determined. Such preliminary reports should remain confidential since they will contain incomplete information. If such reports were to be made public, it would needlessly expose firms to additional risks from bad actors and create confusion for audit clients, particularly because it is not clear how the PCAOB would update reported incidents with newly received information or the determination that the incident has been successfully contained and remediated.

Grant Thornton

Further, if the intent of making incident details public is to provide clients visibility into incidents impacting firms, it should be noted that firms are often already contractually obligated to notify clients of a breach involving client data. Firms and clients are better served by continuing to follow best practices in notifying only those clients who have been impacted and providing tailored communications to those clients.

Timing

In the Proposal, the PCAOB observes that cybersecurity information reported in the past has been "incomplete, inaccurate or insufficiently detailed."[3] However, by requiring the reporting of incidents that have not been confirmed and are in the early stages of investigation, the PCAOB would likely receive more of the same. Firms will rightly be extremely cautious in providing any specific details as long as the incident is still under investigation so as to not to be misleading. Whether the reporting deadline is five business days or another timeframe, if the investigation is still underway and conclusions have not been reached, then the information provided in the incident report would remain indeterminate and unlikely to satisfy the PCAOB's desire for details.

As the PCAOB knows, incident reporting timeframes[4] by covered entities to government agencies are varied and can be as short as 36 hours. Depending on the footprint of an incident, the resulting notification obligations can be voluminous and fast-paced. In the initial stages after a potential incident has been detected, resources are precious, and time is of the essence. At a time when a firm's cyber defense team is seeking to respond and recover,[5] sorting through multiple reporting obligations based on what is reasonably likely to have occurred and may be significant compared to what has actually occurred can divert cyber responders away from their primary objectives (to respond and recover) and to instead focus on applying inconclusive information to various reporting criteria.

This suggests that there is a balance to be struck between the value of immediate reporting versus the value of using limited resources to fully respond to an incident. Because there is no defined role for the PCAOB in assisting a firm in responding to an incident or in defending against an attack, we believe a firm's ability to respond and recover from an incident as promptly as possible should carry more weight than the proposed reporting requirement.

In addition, while the PCAOB may have a regulatory interest in being aware of incidents, such desire for awareness should not outweigh a firm's need to fully devote resources to protecting the confidentiality, integrity, and availability of the systems supporting the firm's operations and the data entrusted to them by clients. Accordingly, where incidents need to be reported, a yearly or quarterly report or, at minimum, 90 days after a confirmed significant cybersecurity incident has actually occurred, would be more suitable timeframes. At that stage, more facts would be available and cyber defense teams would have conducted the vital and time-sensitive

---

[3] Page 9 of the Proposal.
[4] FDIC Final Rule.
[5] See NIST Cybersecurity Framework. Five key functions: Identify, Protect, Detect, Respond, and Recover.

work involved in responding to and recovering from the incident. This suggestion would still permit the PCAOB to receive the information it requires and to conduct necessary follow-ups.

We encourage the PCAOB, in the interest of efficiency, to also consider requiring notification only if a firm is already required to provide notice to a state or federal entity, instead of creating another definition of a cybersecurity incident that requires notice. Firms could be expected to provide the PCAOB with those external notification letters within a certain time period after the letters are distributed to those entities. As a final note, we do not believe it is appropriate to align the proposed requirements with the SEC's requirements for publicly traded entities to report cybersecurity incidents for users to base investment decisions on because the overall use and purpose of this information is ultimately different.

Unintended consequences

We believe that there are potential unintended consequences to the proposed cybersecurity reporting requirements. Creating a new incident reporting requirement for firms adds a layer of complexity and obligation at a time when valuable resources should be dedicated to protecting systems and data by remediating the incident. Firms may already need to consider multiple state and federal laws based on the nature of the incident and the client in addition to their contractual obligations.

Every state has a data breach or cybersecurity incident notification law that may already be directly or indirectly applicable to firms. State laws generally require notification to individuals and/or a designated state entity (for instance, the attorney general) when unauthorized access or acquisition of personal information occurs. In addition, there are state and federal sectoral laws that either directly or indirectly, through client agreements, obligate firms to report data breaches or cybersecurity incidents to clients, government entities, and affected individuals, as applicable. The incident response and reporting space is already heavily populated with obligations, so that creating additional and often repetitive reporting obligations would not be efficient. The PCAOB's proposed approach could create additional risks that run directly contrary to the stated goals of the PCAOB.

Proposed Form QCPP

We understand and appreciate the Board's desire to obtain and retain more updated quality control information from firms, particularly with the Board's recent approval of QC 1000. While we do not believe the new form will be particularly useful to investors or other stakeholders, we do recognize the considerable change from existing quality control requirements that QC 1000 represents for the PCAOB, particularly compared to firms' original Form 1 submissions over 20 years ago. While the core quality control standards of the PCAOB have not changed significantly over the years, firms' application thereof (coupled with the recent adoption of SQMS 1 and ISQM 1, when applicable) has evolved considerably. Therefore, if the Board retains the proposed requirement, it would likely be more efficient for firms to submit a new summary of the proposed quality control information as opposed to summarizing material changes from what was previously reported in Form 1.

We interpret the Form QCPP requirements in the Proposal to be a one-time submission, but it is unclear whether the Board has ongoing expectations or intentions related to updating Form QCPP and requiring additional submissions from accounting firms. If the Board moves forward with this Proposal, we ask it to clarify its intention. We believe that any future submissions of Form QCPP would be unnecessary, particularly considering the rigorous reporting requirements contained within QC 1000.

International considerations

Registered firms from outside the US are subject to various laws and regulations regarding disclosure of personal data and other confidential information. We understand from non-US firms that some of the proposed new required disclosures go beyond what non-US regulators require and may lead to violations of local laws resulting from disclosure of information that non-US auditors are required to keep confidential under: (1) professional secrecy obligations and/or (2) laws and regulations governing disclosure of personal information. In addition, concern has been expressed about the communication and public disclosure of a wide array of sensitive economic and commercial information relating non-US audit firms to a foreign regulator. We anticipate that many non-US firms would seek to decline to provide information based upon conflicts with non-US laws or ask the PCAOB for confidential treatment. Although the Proposal expresses skepticism that disclosure of various items would conflict with applicable non-US law, we believe a better approach would be to allow firms to assert conflicts with non-US laws, which still require those firms to obtain legal opinions to support withholding the information.

Effective date

Appropriate time is necessary in order to sufficiently and appropriately effect change in firms' quality management systems. We do not believe the proposed effective date provides adequate time for firms to undertake the change management necessary to adapt their quality control systems for the requirements, as proposed.

****

We would be pleased to discuss our comments with you. If you have any questions, please contact Jeff Hughes, National Managing Partner of Assurance Quality and Risk, at (404) 475-0130 or Jeff.Hughes@us.gt.com.

Sincerely,

/s/ Grant Thornton LLP