www.CRINDATA.com

May 9, 2022

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

Submitted through the SEC's website portal
To rule-comments@sec.gov,
Subject: File Number S7–09–22

Comment Letter to Proposed Rule

Cybersecurity

Risk Management, Strategy, Governance and Incident Disclosure

SEC RIN: 3235-AM89
File Number S7–09–22

Dear Sir or Madam:

We write in support of the purpose and the direction of, while also providing specific comments and further recommendations with respect to, the abovementioned Proposed rule to require (i) current reporting about material cybersecurity incidents, as well as updates; and (ii) disclosures about risk management, strategy, and governance as related to cybersecurity, as published in 87 Federal Register 16,590, dated March 23, 2022 (the "**Proposed Disclosure Rules**") by the Securities and Exchange Commission, for which comments are requested by May 9, 2022.

I. Preliminary Comment and Focus in Support of the Proposed Rules

We write in overall support of the Proposed Disclosure Rules, with more detailed comments on specific aspects which could make the final rules more efficient and effective for the SEC and industry in support of the SEC's objectives. Requiring more timely and consistent disclosures related to varying aspects of cybersecurity risks and risk management measures are reasonable in light of the importance of such risks to public companies generally, and the benefits to investors and te markets of more timely, consistent and comparable disclosures. In addition to the SEC's goals in promoting transparency, these rules are complementary to the broader objectives of the SEC in understanding and reducing systemic risk, which have led the SEC to require, as well as propose additional rules that would require, reporting to the SEC of operations incidents resulting from cybersecurity or other causes.

While cybersecurity risks are relevant to all public companies in our modern digital age, the impact of analogous incidents at distinct public companies may nonetheless differ substantially as much on the nature of the specific company, its business model, and customer base, as to the level of risk management, strategy and governance put in place *ex ante* to mitigate risks. Moreover, cybersecurity incidents are one component of operational risks that could lead to disruption at public companies, as well as exposure of personal information. Taking into consideration the dependency of public companies generally on third party service providers as described in the proposed rule, the SEC's goals of providing more timely and consistent material information for investors would be better served by focusing more broadly on disclosure of effects of broader operational incidents then the more limited cause of cybersecurity. Finally, the SEC should continue to attempt to harmonize incident reporting with other increasing governmental incident reporting rules.

A. Relation among (i) risk mitigation policies, strategy and governance, and (ii) incident reporting

We generally support the SEC proposing more consistent reporting of cybersecurity risk mitigation measures. We nonetheless note that in proposing greater transparency, the SEC has not proposed to prescribe specific minimum standards or steps as has been the case for regulated financial services providers in connection with a broader compliance program. In such compliance programs implementing policy objectives for the broader financial services sector, it is common to include both proactive risk mitigation measures, as well as disclosures of incidents which occur notwithstanding even reasonable risk mitigation measures. It must be emphasized, however, that disclosures with respect to risk mitigation versus those with respect to incidents are somewhat different.

For current, high-level purposes, we wish to focus on the different temporal nature:

- Policies and procedures are *proactive, ex ante* measures aimed at increasing risk awareness, and where possible risk mitigation, and should be reasonably tailored to the business model and risks of the each public company. It must be noted, however, that while cybersecurity risks may be mitigated through a reasonably designed and implemented program, they cannot be totally eliminated.
- Reporting of incidents is by definition *ex post*, and preparing a structured way for such reporting recognizes that cybersecurity risks may be mitigated but cannot be eliminated. Timely public reporting of material incidents could increase information broadly available to investors.
- Unlike prompt (usually confidential) reporting from a regulated entity to the SEC or other oversight authority, the incident reporting in the Proposed Disclosure Rules are not primarily designed nor would they directly serve to allow the SEC to identify and where possible to act with respect to potential systemic risks to the financial services providers under its oversight. Prompt initial reporting of operational incidents or events may require reporting before the cause is identified, be it *either* due to an "unauthorized occurrence" and hence falling under the proposed cybersecurity incident definition, *or*

some other source of operational failure (e.g., other human error, coding error, hardware failure or natural cause).

- The proposed incident reporting to the public under the Proposed Disclosure Rules should remain secondary to the evolving reporting requirements to public authorities increasingly applicable to many public companies, both in terms of (a) priority of the systemic goals and risk mitigation objectives of the latter reporting; and (b) additional time needed for public companies to assess impact and materiality which would be necessary to make meaningful reporting to the general public under the Proposed Disclosure Rules.

- A further relation between *ex ante* reporting of risk mitigation policies and procedures, cybersecurity governance, etc., and *ex post* reporting of incidents, is that the occurrence of incidents does provide some indication of the reasonableness or effectiveness of an entity's risk mitigation measures, albeit not conclusive indication. An analogy can be made to the principles in the securities industry and related disclosures that risk-taking is correlated with returns (and that additional controls or risk mitigation measures come at costs); as well as that historical return (or historical incidents) are not necessarily indicative of future returns (or incidents).

This comment letter will focus most on elements relevant to the timely reporting of incidents under the Proposed Disclosure Rules. **It would be prudent and consistent with the SEC's goals of making more timely and consistent information to investors not only to adopt cybersecurity incident reporting requirements, but also a broader definition of operations events and incidents reporting, including involving third party service providers, than under the proposed narrow definition of cybersecurity incidents.**

B. Reporting disclosure of effects of operational incidents, versus more narrow disclosure requirements with respect to causes that are cybersecurity incidents

Throughout this comment letter, we note that the SEC's goals of making more timely, consistent and comparable information to investors would be better served by requiring incident reporting with respect to operations disruptions. The SEC has expressed concern over timely reporting by a public company under the proposed rule language that a materiality determination be made "as soon as reasonably practicable after the discovery of the [cybersecurity] incident." This is effectively a two part test of (1) identifying a cybersecurity incident; and (2) determining materiality. In practice, however, a company can be expected in many instances to more quickly be able to identify the ***effect*** of an operational disruption than to discern the ***cause*** as a cybersecurity incident of unauthorized access. This is even moreso the case when the disruption involves an information system "used by the registrant" but operated by a third party service provider, which in the data cited by the SEC in the rulemaking may represent a majority of the cases. The public company can much better assess the impact of a disruption of services from a service provider than it can the cause of the disruption at the service provider. The SEC has made clear in the preamble, and we fully support this, that what constitutes "materiality" for the

purposes of the proposed cybersecurity incidents disclosure would be consistent with existing securities law case law applicable more broadly than cybersecurity.[1] Against that decades of developments of materiality for disclosure to investors, it is even more compelling that the SEC should focus on incident disclosure requirements for operational disruptions more generally, and not narrowly due to cybersecurity causes.

We respectfully suggest that our comments are intended to promote the SEC's goals, and where practical to focus on the most relevant effects of broader operations incidents which in turn would promote more timely, consistent and comparable information for investors.

II. Summary of Conclusion and General Comments

We write in overall support of the proposed rules. This comment letter will provide more detailed comments on the following aspects, which are meant to help the SEC craft rules that will more efficiently and effectively support its objectives.

Requiring cybersecurity risk mitigation disclosures and incident reporting are reasonable in light of the SEC's goals in promoting more timely and consistent information to investors.

Cybersecurity is one of the greatest risks facing not only public companies, but our modern economy more generally, which of course includes customers of public companies and ultimately consumers and investors. That being said, cybersecurity is (i) one component of the broader category of operational risk (i.e., as opposed to more traditional financial sector risks such as credit, market or liquidity risks); and (ii) cybersecurity risks are driven not only by growing cybersecurity threats, but by the exposure created by the increasing reliance on IT and communications, AND, (iii) increasing reliance on third-party service providers including subcontractors. Taking all of the foregoing into consideration, the cybersecurity risk management policies and procedures, and cybersecurity incident reportings should:

- Continue to be part of an overall operational risk management framework and resilience from disruptions leading to a similar negative effect even if not caused by a defined "cybersecurity" incident involving unauthorized access; too narrow or prescriptive cybersecurity rules will lead to a check-the-box approach not consistent with the broader goals and purposes
- Must take into consideration and therefore integrate practices for the public company's oversight of third party service providers
    - Include further expectations for understanding and due diligence of further sub-contracting and further service provider dependency chains
- The requirements for prompt, initial incident reporting should be expanded to apply to operations events beyond just what are initially identified as cybersecurity incidents; otherwise, the public will receive an underreporting of the desired incident information potentially material to investors, and such reporting could be further delayed by the step to evaluate the potential cause of qualification as a cybersecurity incident

[1] See 87 Fed. Reg. at 16,596.

- For incident reporting to be timely and effective, public companies will need to obtain, at least as contractually agreed, timely incident notifications from their service providers, including through subcontractor chains
- The SEC should continue to seek harmonization with reporting of cybersecurity and operational risk incident reporting increasing mandated by the SEC and other government authorities for parties other than public companies (including for public companies due to their regulation as a financial services provider or categorization as part of critical infrastructure)
    - This harmonization also needs to take into consideration that many relevant third party service providers have broader support relationships than just for public companies that might be effected by these Proposed Disclosure Rules
- The recommendations discussed herein have application across public companies of all sizes, and we do not believe that there are significant difference in the relevance, costs, benefits or burdens for public companies based on size that would suggest the need for differing requirements or applicable exemptions. Rather, the nature of the business and risks applicable to a specific public company will be much more relevant than its market capitalization.
- Public companies, including smaller entities, can draw upon industry shared solutions and specialized service providers, both for their oversight of risks—in particular reliance on third party service providers, and in incident reporting. Shared solutions are appropriate and can be viable, effective, and efficient not only at the level of proactive risk mitigation, but throughout the risk management life cycle, and in reporting of incidents, as well as subsequent updates.
- Upon adoption of amended versions of the Proposed Disclosure Rules, the SEC is respectfully requested to withdraw prior guidance which would partially be superseded by such rules, and to re-issue other portions together with revised elements relevant to the new rule framework; specifically, the SEC should withdraw the 2011 Staff Guidance and 2018 Interpretative Release.[2]

III. About the Commenters

This comment is submitted by **CRINDATA**, LLC, (www.CRINDATA.com) which offers solutions to financial institutions for managing operational risk in their reliance on third party service providers. Underlying a significant aspect of the SEC's cybersecurity risk concerns as described in the Proposed Disclosure Rules is the structural framework under which public

[2] We refer to the guidance as described at 87 Fed. Reg. 16,593. The preamble to the proposed rulemaking states: "The guidance set forth in both the 2011 Staff Guidance and the 2018 Interpretative Release would remain in place if the Commission adopts the proposed rule amendments described in this release." *Id.* at 16,594. It creates additional burden to the affected industry members, in this case public companies, to retain guidance that has been at least partially superseded by new rules; retaining these pieces of guidance would increase the burden upon industry and divert resources from focusing on the intended policy goals, thereby also risking undermining effectiveness. As such, a better practice as a regulatory authority would be to withdraw the outdated guidance and restate any elements which the agency wishes to retain beyond the points superseded by a rule implemented from the proposal.

companies rely on a range of distinct service providers in order to operate, which in turn can expose the public company to cybersecurity risks (with the data cited by the SEC suggesting even possibly risks related to a majority of incidents).

CRINDATA offers unique cloud-based solutions to companies, with a focus on high regulated financial institutions who must pro-actively manage their critical third-party relationships (including their indirect relationships with subcontractors) and must prepare for and mitigate business disruption management and cybersecurity events originating anywhere in the chain of service providers and subcontractors. Concurrently, CRINDATA helps third party service providers like cloud providers, payments providers, and transaction monitoring solutions, by substantially simplifying the due diligence interactions with financial service companies and by providing a compliant, common platform and communications to manage business disruptions and cybersecurity events when they occur. The platform serves needs across multiple jurisdictions applying similar, evolving risk management principles. The authors of this comment letter are CRINDATA's co-founders, Mark Stetler and James H. Freis, Jr. Mr. Freis as the primary author draws upon his experience working together with the SEC while serving as Director of the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN), and in a range of other roles on behalf of government and private sector groups including SEC-regulated entities, and in his previously responsibilities as Managing Director at Deutsche Börse AG, where he was responsible for material public disclosures by this blue chip company, as well as aspects of the disclosure requirements for the entities and securities trading on the exchanges operated by the Deutsche Börse Group.

IV. Trend towards operational incident reporting and opportunity to promote further harmonization

While cybersecurity risks are relevant to public companies, they are not in any way unique to them. Rather, the cybersecurity risks are one component of operational risks that could lead to disruption at the public companies, as well as exposure of personal information. Hence, cybersecurity reporting for public companies should be required as part of broader operational event reporting; and harmonized with other increasing governmental incident reporting rules.

Operational events, including cybersecurity incidents, can have implications for investor decision making in terms of direct and indirect costs and adverse consequences including legal risks and the potential for exposure of confidential and/or personal information.[3]

As to relevant operational risks being broader than cybersecurity incidents, the SEC should pursue reporting incident requirements in the broader context of broader operational risk

[3] We agree with the description of costs and adverse consequences mentioned at 87 Fed. Reg. 16,592. We nonetheless note that caution should be made in lumping direct costs (e.g., a cybersecurity incident involving misappropriating assets of a public company) with more speculative negative effects such as whether an event might negatively impact a company's reputation and future business prospects. The securities markets have experience in evaluating probability and materiality, including in connection with accounting standards for impairment or valuations or requiring setting aside reserves.

management efforts. Such broader reporting would be similar to the operational incident reporting that would be required under the SEC's proposed rulemaking to amend Form PF, the confidential reporting form for certain SEC-registered investment advisers to private funds to require current reporting upon the occurrence of key events and other requirements for advisers to certain types of funds, as published in 87 Federal Register 9106, dated February 17, 2022, for which CRINDATA filed a comment letter on March 21, 2022. While the proposed Form PF reporting would be confidential to the SEC, the instant Proposed Disclosure Rules could apply the proposed level of detail, timing, and materiality framework to the broader set of operations events at public companies rather than the more limited definition of cybersecurity incidents.

Reporting of broader operational events including cybersecurity incidents also would be consistent with other SEC initiatives. Reference is made to the notification requirements under the SEC's Regulation Systems Compliance and Integrity (Regulation SCI) which was developed, *inter alia*, in light of the dependency of the securities markets on evolving technology and vulnerabilities to outages including in connection with cyberattacks.[4] Notably, a covered entity is required both to make an "immediate" notification to its Federal regulator of an incident; followed within 24 hours on a "good faith, best efforts basis" by a notification of event and assessment to the extent available at that time; and at later times more detailed impact assessments.[5] The SEC also has published for comment a proposed rule that would to require registered investment advisers and investment companies to adopt and implement written cybersecurity policies and procedures reasonably designed to address cybersecurity risks, and to report significant cybersecurity incidents,[6] for which CRINDATA also filed a public comment letter on April 11, 2022.

Particularly instructive for the SEC, and essential for efforts of the Financial Stability Oversight Council to monitor potential systemic risks, should be the new reporting requirement effective May 1, 2022 by the U.S. Federal Banking Agencies – the Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, and Federal Deposit Insurance Corporation.[7] That final rule requires a banking organization to notify its primary Federal regulator of any ''computer-security incident'' that rises to the level of a ''notification incident,'' as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred. The final rule also requires a bank service provider to notify each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has caused, or is reasonably likely to cause, a material service disruption or degradation for four or more hours. Notably, the Federal Banking Agencies require incident reporting broader than cybersecurity incidents and more akin to the SEC policy's concern underlying the proposed operations events reporting on

[4] See SEC Final Rule, Systems Compliance and Integrity, 79 Fed. Reg. 72,252 (December 5, 2014), as implemented in particular in 17 CFR § 242.1002--.1007, available at 2014-27767.pdf (govinfo.gov). The primary author of this comment letter previously had oversight responsibility for the implementation of Regulation SCI by SEC regulated exchanges.
[5] See 17 CFR § 242.1002(b).
[6] See 87 Fed. Reg. 13,524 (March 9, 2022).
[7] See 86 Fed. Reg. 66,424 (November 23, 2021).

funds PF. This is made clear in the background explanation of the final rule of the Federal Banking Agencies, but is equally relevant to the SEC's policy objectives underlying the Proposed Rules for advisers and funds: "Computer-security incidents can result from destructive malware or malicious software (cyberattacks), as well as non-malicious failure of hardware and software, personnel errors, and other causes."[8]

The trend to require additional reporting of incidents or operations events will only continue. After the SEC's March 9, 2022 announcement of the Proposed Disclosure Rules, on March 15, 2022 the President signed into law the Consolidated Appropriations Act, 2022.[9] That appropriations law also contains the ''Cyber Incident Reporting for Critical Infrastructure Act of 2022" which authorizes rulemaking for incident reporting across a broad range of actors (including components of the financial sector) and calls for coordination with any analogous reporting requirements by other government agencies. Other jurisdictions are following analogous paths to mandate incident reporting. One prominent example is the European Union's proposed Digital Operations Resilience Act (DORA),[10] for which a revised proposal after a round of public consultation is expected soon.

This broader context should be understood as strong support for the policy goal of the SEC requiring additional reporting of relevant operations events including cybersecurity incidents, and in moving forward with additional reporting requirements without delay. That notwithstanding, the broader trend towards such reporting also emphasizes the need for the SEC to take an approach more consistent across the SEC's own various new reporting proposals. The broader trend also suggests that the SEC should attempt to act increasingly consistently with other governmental authorities for which there is not a differing policy goal or interest. **Many public companies that would be impacted by the Proposed Disclosure Rules are also subject to the above current or soon to be expected additional reporting requirements. Moreover, many underlying entities impacted by the reporting requirements—in particular third party service providers—support multiple different regulated entities.** Analogous goals requiring nonetheless different prescriptive reporting methods, formats, data fields and timing would make more difficult the goals sought by the SEC and a range of other government entities to obtain and be able to share information about incidents and potential indicators of systemic risks; it would also raise the complexity and costs, and make more difficult for the regulated industry to timely notify reportable incidents. Again, a relevant consideration is that the parties involved in reportable incidents often will include broader IT service providers and sub-contractors that are not limited to the Proposed Disclosure Rules at issue here for public companies; rather an operations event or incident affecting an entity such as a cloud services provider (of which the leaders are large public companies) could in the future

[8] See id. at 66,425 (emphasis added).
[9] Public Law No: 117-103 (March 15, 2022).
[10] See Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, available at EUR-Lex - 52020PC0595 - EN - EUR-Lex (europa.eu).

trigger directly or indirectly through affected chains of customers, reporting to a broad range of government entities.

From a timing perspective, we submit that deadlines for timely reporting should follow this general order of priority, which should be maintained in relevant order even where specific time thresholds might be adopted, and this reporting should be with respect to *effects* of disruptions beyond limited cybersecurity *causes*:

- **Prompt reporting of third party service providers of disruptions to the companies that they support**, prior to having made a detailed analysis of either cause or potential materiality
- **Prompt reporting of operations events by critical infrastructure or designated industry sectors to competent government authorities on a confidential basis**, subject to a basic materiality standard but without detailed analysis of either cause or potential effect
- **Upon materiality determination, further reporting or update to government authorities as well as contractual counterpart companies** who might be affected
- **Public company reporting based on materiality to general public** for relevance in investment decisions
- **Reporting to individual affected consumers**, such as with respect to data breach.

Part of harmonization, increased effectiveness towards the systemic risk mitigation goals of the SEC and other governmental authorities, and achieving these goals in a more efficient, effective, and less costly way for entities subject to reporting obligations would be to allow operational risk mitigation information sharing and incident reporting on behalf of these entities by specialized service providers acting on their behalf.

V. Specific Comments and Responses to Request for Comment Questions

The following responds in more detail to some of the specific items on which comments were requested in connection with the proposed rules.

1. Would investors benefit from current reporting about material cybersecurity incidents on Form 8-K? Does the proposed Form 8-K disclosure requirement appropriately balance the informational needs of investors and the reporting burdens on registrants?

Yes, investors would benefit from more timely reporting about material cybersecurity incidents. More relevant information would be provided to investors on a more timely basis, if the reporting requirement were related to operational events or disruptions rather than the more narrow definition of cybersecurity incidents, as explained throughout this comment letter.

2. Would proposed Item 1.05 require an appropriate level of disclosure about a material cybersecurity incident? Would the proposed disclosures allow investors to understand the nature of the incident and its potential impact on the registrant, and make an informed investment decision? Should we modify or eliminate any of the specified disclosure items in proposed Item 1.05? Is there any additional information about a material cybersecurity incident that Item 1.05 should require?

Additional relevant information that should be included is the extent to which the material operational disruption (caused by a cybersecurity incident or otherwise) occurred primarily at the reporting company or at a third party service provider.

4. We are proposing to require registrants to file an Item 1.05 Form 8-K within four business days after the registrant determines that it has experienced a material cybersecurity incident. Would the proposed four-business day filing deadline provide sufficient time for registrants to prepare the disclosures that would be required under proposed Item 1.05? Should we modify the timeframe in which a registrant must file a Form 8-K under proposed Item 1.05? If so, what timeframe would be more appropriate for making these disclosures?

As described on the preceding page, it is important that the timing first take into consideration appropriate priorities as compared to other aspects of evolving incident reporting obligations. Provided that such prioritization can be maintained, the period of four days from a materiality determination seems reasonable for a public company to report, while still making information available to an investor much earlier than the current practice as described anecdotally in the preamble to the rule. It should be noted that a materiality determination and the preparation of a public disclosure will require input from persons of various backgrounds, likely including cybersecurity experts, legal counsel, investor relations, and business area leaders, thus requiring some time to coordinate an appropriate public disclosure.

5. Should there be a different triggering event for the Item 1.05 disclosure, such as the registrant's discovery that it has experienced a cybersecurity incident, even if the registrant has not yet been able to determine the materiality of the incident? If so, which information should be disclosed in Form 8-K based on a revised triggering event? Should we instead require disclosure only if the expected costs arising from a cybersecurity incident exceed a certain quantifiable threshold, e.g., *a percentage of the company's assets, equity, revenues or net income or alternatively a precise number? If so, what would be an appropriate threshold?*

The SEC should consider adopting in addition to the requirement of disclosing an incident material to the public company as a whole, to also require disclosure of an incident material to a segment already defined in the company's public reporting. For example, if the public company is a conglomerate with three separate business lines, each with its own profit and loss statement and running somewhat independently, and already described as such in separate segment reporting, then the company might be expected to report an operational incident that is material to a specific segment even if it could be argued that the expected impact of the incident might not be considered material for the company as a whole.

6. To what extent, if any, would the proposed Form 8-K incident reporting obligation create conflicts for a registrant with respect to other obligations of the registrant under federal or state law? How would any such conflicting obligations arise, and what mechanisms could the Commission use to ensure that registrants can comply with other laws and regulations while providing these timely disclosures to investors? What costs would registrants face in determining the extent of a potential conflict?

Adopting a priority of reporting as described two pages preceding would help reduce potential conflicts for different reporting obligations.

8. We are proposing to include an instruction that "a registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident." Is this instruction sufficient to mitigate the risk of a registrant delaying a materiality determination? Should we consider further guidance regarding the timing of a materiality determination? Should we, for example, suggest examples of timeframes that would (or would not), in most circumstances, be considered prompt?

The proposed rule language is that a materiality determination be made "as soon as reasonably practicable after the discovery of the [cybersecurity] incident." This is effectively a two part test of (1) identifying a cybersecurity incident; and (2) determining materiality. In practice, however, a company can be expected in many instances to more quickly be able to identify the ***effect*** of an operational disruption than to discern the ***cause*** as a cybersecurity incident of unauthorized access. This is even moreso the case when the disruption involves an information system "used by the registrant" but operated by a third party service provider, which in the data cited by the SEC in the rulemaking may represent a majority of the cases. The public company can much better assess the impact of a disruption of services from a service provider than it can the cause of the disruption at the service provider. The SEC has made clear in the preamble, and we fully support this, that what constitutes "materiality" for the purposes of the proposed cybersecurity incidents disclosure would be consistent with existing securities law case law applicable more broadly than cybersecurity.[11] Against that decades of developments of materiality for disclosure to investors, it is even more compelling that the SEC should focus on incident disclosure requirements for operational disruptions more generally, and not narrowly due to cybersecurity causes.

Yes, it would be useful is the SEC were to suggest examples of timeframes that would (or would not) be considered prompt.

10. As described further below, we are proposing to define cybersecurity incident to include an unauthorized occurrence on or through a registrant's "information systems," which is proposed to include "information resources owned or used by the registrant." Would registrants be reasonably able to obtain information to make a materiality determination about cybersecurity incidents affecting information resources that are used but not owned by them? Would a safe

[11] See 87 Fed. Reg. at 16,596.

harbor for information about cybersecurity incidents affecting information resources that are used but not owned by a registrant be appropriate? If so, why, and what would be the appropriate scope of a safe harbor? What alternative disclosure requirements would provide investors with information about cybersecurity incidents and risks that affect registrants via information systems owned by third parties?

One of the greatest challenges for public companies, or any company relying on third party services providers including a potential further chain of subcontractors, is to receive timely information about incidents involving such service provider or subcontractors. That being said, the standard for reporting by the public company should be a material *effect* on the public company, regardless of the *cause*. Thus, the SEC should be clear that the definition of information systems is meant to recognize that some such systems may rely on external service providers, but the materiality is nonetheless with respect to the effect on the public company. The public company can in most aspects determine such materiality even where the initial impact is with a service provider. There may be notable exceptions to this ability to determine, such as if personal data were breached at a service provider without a noticeable operational impact on the public company. The only way to reconcile such cases is for SEC to have an expectation that the public company will oversee its external service providers engaged in material services (those relevant to potential material risks) and include at least a contractual requirement of notification from the service provider to the public company of a potentially material incident at the service provider or a subcontractor (which in turn requires notification of incidents from the subcontractor to the service provider).

As described throughout this comment letter, requiring public companies to describe material disruptions from operational incidents of a broader nature, rather than more limited to a cybersecurity cause, would be an alternative disclosure requirement better benefitting investors.

Any public company should have a risk assessment as to its operational dependencies upon service providers. Such risk assessment should also take into consideration whether the third party has critical dependencies on underlying sub-contractors or other service providers, in which case such underlying parties should also be included in the risk assessment.

No, a safe harbor for information about cybersecurity incidents affecting information resources that are used but not owned by a registrant would <u>not</u> be appropriate? Particularly in light of the limited evidence cited by the SEC that perhaps a majority of cybersecurity incidents derive from service provider relationships, such a safe harbor would vitiate the purposes of the rule. Rather, the materiality assessment already accounts for the information asymmetry in that the public company can only assess materiality after it becomes aware of incident, and only thereafter would reporting obligations apply. For the benefit of investors, public companies should be expected to adopt reasonable measures to obtain more timely information from their most critical service providers. There is amply experience in this regard from the regulated financial services industry, including in connection with the evolving service provider oversight and incident reporting requirements referenced, *supra*, at pages 7 to 8 of this comment letter.

12. We note above a non-exclusive list of examples that would merit disclosure under Item 1.05 of Form 8-K covers some, but not all, types of material cybersecurity incidents. Are there additional examples we should address? Should we include a non-exclusive list of examples in Item 1.05 of Form 8-K?

Yes, a non-exclusive list of examples should be included in Form 8-K. This would promote uniformity and the ability of investors to compare different public companies, as well as to better analyze various incidents which may occur over time.

15. Should we require registrants to disclose any material changes or updates to information that would be disclosed pursuant to proposed Item 1.05 of Form 8-K in the registrant's quarterly or annual report, as proposed? Are there instances, other than to correct inaccurate or materially misleading prior disclosures, when a registrant should be required to update its report on Form 8-K or file another Form 8-K instead of providing disclosure of material changes, additions, or updates in a subsequent Form 10-Q or Form 10-K?

Yes, updates of material information should be disclosed to avoid information being misleading. This is particularly the case about a negative developments – it will commonly be the case that early reporting with not be able reasonably to determine the potential negative costs or adverse consequences of an incident. Other aspects of the type of disclosure to be provided, for example from the non-exclusive list "any changes in the registrant's policies and procedures as a result of the cybersecurity incident…"[12] should not be expected to require amended disclosures, but rather could be provided in the next quarterly reporting.

17. Should we adopt Item 106(b) and (c) as proposed? Are there other aspects of a registrant's cybersecurity policies and procedures or governance that should be required to be disclosed under Item 106, to the extent that a registrant has any policies and procedures or governance? Conversely, should we exclude any of the proposed Item 106 disclosure requirements?

The preamble to the proposed rulemaking states: "Given that a significant number of cybersecurity incidents pertain to third party service providers, the proposed rules would require disclosure concerning a registrant's selection and oversight of third-party entities as well."[13] The language with respect to third party service provider oversight is too narrow, in that it is limited to cybersecurity aspects. More appropriately, cybersecurity risk is only one component of an operational risk review of relying on a third party service provider.

Additionally, one of the most important provisions for effective risk assessment and oversight of service providers for operational risk management (including, but not limited to cybersecurity risks), is for the adviser or fund to have transparency with respect to material dependencies of the service provider on further subcontractors or other service providers to the service providers (also sometimes referred referred to as fourth parties). Because, by definition, there is no contractual privity between the adviser or fund and a "fourth party," there is a reliance on the

[12] See 87 Fed. Reg. at 16,598, bottom of right column.
[13] 87 Fed. Reg. at 16,599 (footnote omitted).

third party to oversee and provide information with respect to the fourth party, including changes to the use of different material fourth parties.

As related to incident reporting, if a significant incident impacts a fourth party, there must be not only contractual agreements in place, but also structured reporting mechanisms, to allow the reporting of relevant incident information:

- from the fourth party (or further chain of subcontractors up the chain) to the third party
- from the third party to the adviser or fund
- from the regulated adviser or fund to the SEC as regulator, as well as any other applicable authority.

Understanding and assessing risks, and getting notification of incidents in timely fashion, from fourth parties or other third party service provider chains are among the greatest challenges faced for public companies. A shared solution or type of utility serving multiple companies lends itself well to sharing costs and more efficiently leveraging risk management solutions. CRINDATA is a provider of one such shared solution.

It is suggested that the SEC not be prescriptive, but rather raise awareness such as in guidance on best practices about the importance of understanding exposure and addressing information needs on third party providers and their subcontractors or fourth parties. Analogous approaches have been expected for years by the Federal Banking Agencies, and revisions to guidance on oversight of outsourcing to third parties have recently been published for public consultation.[14]

18. Are the proposed definitions of the terms "cybersecurity incident," "cybersecurity threat," and "information systems," in Item 106(a) appropriate or should they be revised? Are there other terms used in the proposed amendments that we should define?

While the definitions of "cybersecurity threat" and related terms appear largely sufficient for the purpose of the proposal to adopt cybersecurity policies and procedures, the term "cybersecurity incident" is too narrow for the incident reporting requirement. Rather, the SEC should introduce a broader definition of reportable operations events or incidents including cybersecurity-related incidents.

The proposed definition of "cybersecurity incident" is:

> Cybersecurity incident means an unauthorized occurrence on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein.

Thus, a reportable incident would be one that involves an "unauthorized occurrence." In practice, many "unauthorized occurrences" such as malware or trojans may go undetected for some time after being introduced, or, it may take time for the source of a disruption event to be detected and identified as to whether it was caused by an "unauthorized occurrence." Various other aspects of the definitions and the preamble to the Proposed Rules make clear that the

[14] See Proposed Interagency Guidance as published in 86 Federal Register 38,183 (July 19, 2021).

purpose of the proposed incident reporting should not be limited to the cybersecurity *cause*, but rather that the concerns are with respect to the *effects* an incident could have on "confidentiality, integrity, or availability." Thus, the SEC, should wish reporting to include disruptions which appear likely to affect "confidentiality, integrity, or availability."

It is suggested that the SEC adopt for the purposes of a new incident reporting requirement a definition of a reportable Operations Event that would be the same as that which it adopts in connection with its pending proposal, mentioned above, for reporting by private funds: that the registrant experiences a significant disruption or degradation of the reporting entity's key operations, whether as a result of an event at a service provider or the public company.

In conclusion, whatever the final definition of a reportable incident, it is in the interest of the SEC and its goals of promoting the availability of more timely and consistent information to investor about material risks to have more operations incidents reported, rather than risking more narrow reporting based on whether the reporting entity has timely identified a more narrow causation involving an "unauthorized occurrence."

24. Should we provide for delayed compliance or other transition provisions for proposed Item 106 for certain categories of registrants, such as smaller reporting companies, emerging growth companies, FPIs, or asset-backed securities issuers? Proposed Item 106(b), which would require companies to provide disclosures regarding existing policies and procedures for the identification and management of cybersecurity incidents, would be required in annual reports. Should the proposed Item 106(b) disclosures also be required in registration statements under the Securities Act and the Exchange Act?

No. The recommendations discussed herein have application across public companies of all sizes, and we do not believe that there are significant difference in the relevance, costs, benefits or burdens for public companies based on size that would suggest the need for differing requirements or applicable exemptions. Rather, the nature of the business and risks applicable to a specific public company will be much more relevant than its market capitalization.

50. Are there any other alternative approaches to improve disclosure of material cybersecurity incidents, cybersecurity risk management, strategy, or governance that we should consider? If so, what are they and what would be the associated costs or benefits of these alternative approaches?

With respect to incident disclosures, as discussed throughout this comment letter, a better alternative to more narrow reporting based on a determined cybersecurity cause would be to require reporting of material disruptions to a public company arising from a broader range of operational events or incidents. Such broader disclosure would come without much additional costs, would potentially be more timely, and would provide more material information to investors and this be of great benefit to investors.

VI. Closing

Thank you for the opportunity to comment on the Proposed Disclosure Rules, and in particular with respect to incident reporting that could better further the SEC's goals of providing more timely and consistent information to investors if incorporated as part of a broader reporting of material operations events or incidents.

Sincerely,

CRINDATA, LLC

By: *James H. Freis, Jr.*
James H. Freis, Jr.
Co-Founder & Chairman

Mark Stetler
Mark Stetler
Co-Founder & CEO