INSIGHTS

The Corporate & Securities Law Advisor

VOLUME 37, NUMBER 10, OCTOBER 2023

Wolters Kluwer

www.WoltersKluwerLR.com

INSIGHTS

The Corporate & Securities Law Advisor

Editor-in-Chief
BROC ROMANEK
broc.romanek@gmail.com

EDITORIAL ADVISORY BOARD

EDITORIAL OFFICE
28 Liberty Street,
New York, NY 10005
212-771-0600

Wolters Kluwer
Richard Rubin, Publisher
Jayne Lease, Managing Editor

INSIGHTS (ISSN No. 0894-3524) is published monthly by Wolters Kluwer, 28 Liberty Street, New York, NY 10005. To subscribe, call 1-800-638-8437. For customer service, call 1-800-234-1660 or visit www.wolterskluwerlr.com.

For article reprints and reprint quotes contact *Wrights Media* at 1-877-652-5295 or go to *www.wrightsmedia.com.*

www.WoltersKluwerLR.com

CYBERSECURITY

Preparing for New Cybersecurity Disclosures

By Meredith B. Cross, Jonathan Wolfman, Alex Bahn, Lillian Brown, Kirk J. Nahra, and Benjamin A. Powell

Public companies will soon be required to provide increased transparency about cybersecurity incidents, risk management, strategy and governance as a result of new rules adopted by the Securities and Exchange Commission (SEC or Commission) on July 26, 2023.[1] These new disclosure requirements represent a significant expansion of the existing SEC disclosure guidance, which dates back to 2011 and 2018, and represent the SEC's first disclosure requirements explicitly referring to cybersecurity risk and incident reporting in current and periodic reports.

Following an overview of the new rules, we identify practical considerations for registrants in preparing for the new disclosure requirements.

Background

Previously, cybersecurity risk and incident disclosures in SEC reports were informed primarily by SEC Staff guidance published in 2011 (2011 Staff Guidance) and Commission level guidance published in 2018 (2018 Interpretive Guidance). In the 2011 Staff Guidance, the SEC Division of Corporation Finance Staff acknowledged that although there were no disclosure rules explicitly referring to cybersecurity risks and incidents, registrants may be obligated to disclose such risks and incidents, as well as material information regarding such risks and incidents, when making other required disclosures pursuant to obligations under existing rules, such as Regulation S-K Items 101 (description of business), 103 (legal proceedings), 105 (risk factors), 303 (management's discussion and analysis of financial condition and results of operation), and 307 (disclosure controls and procedures), as well as certain provisions in the Accounting Standards Codification.[2]

The 2018 Interpretive Guidance added to the SEC Staff's prior guidance on cybersecurity disclosures by discussing potential reporting obligations under Regulation S-K Item 407 (corporate governance), Regulation S-X and Regulation FD, noting that registrants may provide current reports to maintain the accuracy and completeness of effective shelf registration statements and encouraging companies to consider whether insider trading restrictions should be put into effect following a cybersecurity incident and before disclosure surrounding such incident is made.[3]

On March 9, 2022, the SEC proposed new rules to increase and standardize cybersecurity disclosures by public companies subject to reporting requirements under the Securities Exchange Act of 1934, as amended (the Exchange Act).[4] The SEC reopened the comment period on the proposal twice and received over 150 comment letters. Commenters raised various concerns about the rule proposals, with a significant number of comments concerning the timing of the proposed incident disclosure requirement in particular, as well as the proposed board expertise disclosure requirement.[5]

On July 26, 2023, in a 3-2 vote, the SEC adopted new rules for public companies that require current reporting of material cybersecurity incidents, as well as annual disclosures about cybersecurity risk management, strategy, and governance. The new rules and

Meredith B. Cross, **Jonathan Wolfman**, **Alex Bahn**, **Lillian Brown**, **Kirk J. Nahra**, *and* **Benjamin A. Powell** *are attorneys of Wilmer Cutler Pickering Hale and Dorr LLP.* *The authors want to thank the contributions of Nickolas Andreacchi, Amy M. Gopinathan, and Alan J. Wilson to this article.*

amendments affect Forms 8-K, 6-K, 10-K, and 20-F, and include inline XBRL tagging requirements.[6] The new requirements apply broadly to all public companies, including foreign private issuers, emerging growth companies and smaller reporting companies.

The new rules will significantly affect the way public companies disclose cyber incidents and matters relating to their cybersecurity oversight. In adopting the new requirements, the SEC confirmed that the 2018 Interpretive Release and 2011 Staff Guidance remain applicable and should be used to inform potential disclosure obligations relating to cyber incidents that are not specifically addressed in the latest rule requirements.[7]

The implementation dates under the new rules, which are outlined in the chart set out subsequently in the article, are extremely tight. In general, companies other than smaller reporting companies will be required to comply with the new current reporting requirements in Forms 8-K and 6-K beginning December 18, 2023. Smaller reporting companies will be subject to the new current reporting requirements on June 15, 2024. For all companies, the annual reporting requirements in Forms 10-K and 20-F will apply starting with their Forms 10-K and 20-F filed in early 2024.

Summary of New Disclosure Requirements in Current Reports

The new rules establish a real-time reporting requirement for material cybersecurity incidents. This generally applies separately and in parallel with any other cyber reporting obligations the registrant is subject to under federal, state, or foreign law.

Amendments to Form 8-K

Under new Item 1.05 of Form 8-K, a registrant that experiences a material cybersecurity incident must report the "material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations."

In response to public comment about the scope of the new rule, the SEC indicated that it adopted this language in an attempt to better focus the disclosure on the effects of a material cybersecurity incident, rather than specific details regarding the incident itself. Notably, in a departure from the proposal, the final rule does not require companies to discuss the cybersecurity incident's remediation status, if it is ongoing, or whether data were compromised. Nor does the rule require disclosure of the specific or technical information about the registrant's planned response or its cybersecurity systems, networks and devices, or potential system vulnerabilities to such a degree of detail as would impede the registrant's response or remediation of the incident.

Cybersecurity Incident

For disclosure purposes, a "cybersecurity incident" is defined as "an unauthorized occurrence, or a series of related unauthorized occurrences, 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." The "series of related unauthorized occurrences" language reflects the SEC's stated view that "cybersecurity incident" should be viewed broadly. This language is a change from the proposal, which would have required disclosure in periodic reports when it became known to management that a series of previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate.[8]

The adopting release includes examples of situations that may trigger Item 1.05 disclosure, including incidents occurring on third-party systems or accidental exposures of customer data that results in unauthorized access to that data.[9] This same definition of cybersecurity incident and broad interpretation applies to Item 1.05 of Form 8-K as it does for purposes of the disclosures provided pursuant to Regulation S-K Item 106 (discussed below).

Third-Party Service Providers

Registrants are not exempt from providing disclosures regarding cybersecurity incidents on third-party

systems they use, nor will they receive a safe harbor for information disclosed about third-party systems they use. Depending on the circumstances of a cybersecurity incident that occurs on a third-party system, disclosures may be required by either or both of the service provider and customer. Because the definition of "information systems" covers electronic information resources "owned or used by the registrant," a registrant is required to disclose a cybersecurity incident suffered by a third-party information technology service provider's system in a current report on Form 8-K if such incident has a material impact on the registrant.

The SEC noted in the adopting release that registrants need only disclose information made available to them, and generally are not required to conduct additional inquiries beyond their regular communications with third-party service providers pursuant to those contacts and in accordance with such registrant's disclosure controls and procedures.[10] With this in mind, we recommend that registrants carefully review their policies and procedures with respect to oversight of third-party systems.

Materiality

Disclosure is required under Item 1.05 of Form 8-K only if the registrant determines that the cybersecurity incident it experienced is "material." Whether a cybersecurity incident is "material" is to be analyzed under the traditional securities law definition of materiality, meaning an incident is material if "there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision, or if it would have "significantly altered the 'total mix' of information made available." Registrants must consider both qualitative and quantitative factors when assessing the materiality of a cybersecurity incident.[11]

Timing of Disclosure and Permitted Delays

An Item 1.05 Form 8-K must be filed within four business days of a registrant determining it has experienced a material cybersecurity incident. Per Instruction 1 to Item 1.05, a registrant's materiality determination must be made without unreasonable delay after discovery of the incident. This timing standard is a change from the proposal, which would have required the materiality determination to be made "as soon as reasonably practicable after discovery of the incident." The adopting release includes examples of what would constitute "unreasonable delay," including when intentionally delaying a board or committee meeting on the materiality determination past the normal time it takes to convene its members, or revising policies and procedures to delay a determination by extending the registrant's incident severity assessment deadlines.

At the Open Meeting of the SEC held July 26, 2023, Chair Gensler emphasized that the four-business day period to file an Item 1.05 Form 8-K begins when a registrant determines a cybersecurity incident is material, rather than when the registrant discovers that the cybersecurity incident occurred and/or is ongoing.[12]

In response to public comments raising concerns with the four-business day deadline, the SEC added paragraph (c) to Item 1.05, which allows for delayed Form 8-K reporting in extremely limited circumstances. Registrants may delay filing an Item 1.05 Form 8-K when the US Attorney General determines that disclosure under Item 1.05 poses a substantial risk to national security or public safety, and the Attorney General notifies the SEC of such determination in writing.

Under these circumstances, the registrant may delay providing an Item 1.05 Form 8-K filing for the time period specified by the US Attorney General, which may be up to 30 days from the date when the disclosure under Item 1.05 was otherwise required, subject to an additional extension period of up to another 30 days. In extraordinary circumstances involving national security (but not public safety), a further extension for an additional period of up to 60 days may be available. If the Attorney General indicates that further delay is necessary, the SEC will consider such request and may grant such relief through a Commission exemptive order.

A registrant will be notified by the Department of Justice whenever the Attorney General communicates a determination to the SEC so that such registrant may delay filing its Form 8-K. Based on written statements from the Federal Bureau of Investigation (FBI), additional guidance from that agency and the Department of Justice concerning the intake and evaluation process for requests to delaying filing for reasons of national security or public safety is anticipated in the weeks and months ahead.

In response to public comments regarding conflicts with other Federal laws and regulations, the SEC added paragraph (d) to Form 8-K Item 1.05, which also allows delayed 8-K reporting in certain circumstances. Specifically, registrants may delay filing an Item 1.05 Form 8-K where the data breach involves customer proprietary network information (CPNI) that must be disclosed pursuant to certain rules of the Federal Communications Commission (FCC). Registrants covered by 47 C.F.R. § 64.2011 are required to notify the United States Secret Service (USSS) and the FBI no later than seven business days after reasonable determination of a CPNI breach and to refrain from notifying customers or disclosing the breach publicly until seven business days after the USSS and FBI were notified.

Because of this, paragraph (d) allows registrants to delay making an Item 1.05 Form 8-K report up to seven days after the USSS and FBI are notified of a data breach involving CPNI covered by the applicable FCC regulations, provided that written notification is given to the SEC by the date disclosure required by Item 1.05 was otherwise required to be made.

The new rules require foreign private issuers to furnish on Form 6-K information about material cybersecurity incidents that they disclose or otherwise publicize in a foreign jurisdiction, to any stock exchange, or to security holders. This reporting requirement is consistent with other items that foreign private issuers are required to report on Form 6-K. Unlike reports under Item 1.05 of Form 8-K, Form 6-K does not include a four-business day reporting deadline.

Amending Prior Item 1.05 Form 8-K Disclosures

The SEC acknowledged in its adopting release that certain information responsive to the requirements of new Item 1.05 may not be determined or might be unavailable at the time the Item 1.05 Form 8-K is required to be filed.[13] In response to public comments, the SEC revised Instruction 2 to Item 1.05, which now provides that whenever a registrant determines information required to be disclosed under Item 1.05 is not available or determined at the time of the required filing, then the registrant must (1) include a statement to this effect in its Item 1.05 Form 8-K, and (2) within four business days after the registrant, without unreasonable delay, determines such information or such information becomes available, file an amendment to the initial Item 1.05 Form 8-K. This is a change from the proposed rule, which would have required updated incident disclosure in companies' periodic reports.[14]

Amendments to the Eligibility of Provisions of Form S-3 and Form SF-3 and Safe Harbor Provisions in Exchange Act Rules 13a-11 and 15d-11

Similar to other Form 8-K items that rely on materiality determinations, a registrant's untimely filing of an Item 1.05 Form 8-K will not result in a loss of Form S-3 or SF-3 eligibility. Further, Rules 13a-11 and 15d-1 have been amended to include new Item 1.05 of Form 8-K in the list of Form 8-K items eligible for a limited safe harbor from liability under Section 10(b) of and Rule 10b-5 under the Exchange Act.

Summary of New Disclosure Requirements in Periodic Reports

The rule amendments add new Item 106 to Regulation S-K, which requires enhanced and standardized disclosure of registrants' cybersecurity risk management, strategy, and governance. New Item 106 disclosures will be required to be reported in annual reports on Form 10-K, whether or not similar information will be included in a registrant's proxy

statement in the discussion of cybersecurity oversight or otherwise. Similar disclosure requirements were added to Form 20-F as new Item 16K.

Amendments to Forms 10-K

New Item 1C to Form 10-K directs registrants to provide the information required by new Item 106 of Regulation S-K. At a high level, registrants must disclose:

- Company processes, if any, to assess, identify, and manage material cybersecurity risks;
- Management's role and expertise in assessing and managing material cybersecurity risks; and
- Board of directors' oversight of cybersecurity risks.

Risk Management and Strategy

Pursuant to new Item 106(b) of Regulation S-K, a company must disclose their processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats. Such disclosures must be provided in sufficient detail for a reasonable investor to understand such processes. New Item 106(b)(1) includes the following non-exhaustive list of disclosure items a registrant should address:

- Whether and how any of the cybersecurity processes have been integrated into such registrant's overall risk management system or processes;
- Whether and how, in connection with a registrant's cybersecurity processes, such registrant engages assessors, consultants, auditors, or other third parties; and
- Whether the registrant has processes to oversee and identify certain risks from cybersecurity threats associated with its use of any third-party service provider.

In addition to the items above, the SEC stated in its adopting release that "registrants should additionally disclose whatever information is necessary, based on their facts and circumstances, for a reasonable investor to understand their cybersecurity processes."[15] Notably, in response to some commenters, the SEC clarified in the adopting release that disclosure about third-party service providers need not name the specific third parties nor describe the services that they provide.[16]

The final rules also add new Item 106(b)(2) of Regulation S-K, which requires a registrant to disclose in its annual report a description of "whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant, including its business strategy, results of operations, or financial condition and if so, how."[17]

Governance

Pursuant to new Item 106(c) of Regulation S-K, a registrant will be required to disclose the board's oversight of risks from cybersecurity threats and management's role and expertise in assessing and managing material risks from cybersecurity threats. In a departure from the proposed rule, disclosure as to a registrant's board of directors' cybersecurity expertise is not required.[18]

Specifically, Item 106(c)(1) of Regulation S-K will require a description of a registrant's board of directors' oversight of risks posed by cybersecurity threats and, if applicable, identification of any committee or subcommittee of the board responsible for cybersecurity risk oversight and a description of the processes by which the board or applicable committee is informed about risks from cybersecurity threats. The SEC noted in its adopting release that, despite comments to the contrary, Item 106(c)(1) serves a distinct purpose from the existing Item 407(h) requirement that a company disclose its board's leadership structure and administration of risk oversight generally.[19]

Item 106(c)(2) of Regulation S-K will require a registrant to disclose annually management's role in managing and assessing the registrant's material risks from cybersecurity threats. The rule provides the following non-exclusive list of disclosure items a registrant should address in disclosing such role by their management:

- Whether and which management positions or committees are responsible for assessing and

managing risks from cybersecurity threats, and the relevant expertise of such persons;
- The processes by which such persons or committees become informed of and monitor the prevention, detection, mitigation and remediation of cybersecurity incidents; and
- Whether such persons or committees report information about such risks to the board of directors (or any committee or subcommittee).

The discussion of the relevant experience of persons responsible for assessing and managing cybersecurity risk must be in such detail as "necessary to fully describe the nature of the expertise." Instruction 2 to Item 106(c) states that such discussion may include prior cybersecurity work experience, any relevant degrees or certifications, or any knowledge, skills or additional background in cybersecurity.

Definitions

New Item 106(a) of Regulation S-K contains definitions for the following terms as they appear in that section: cybersecurity incident, cybersecurity threat, and information systems. As discussed above, the definition of "cybersecurity incident" was revised from the proposal to include the phrase "series of related unauthorized occurrences," to reflect the SEC's view that "a series of related occurrences may collectively have a material impact or reasonably likely material impact and therefore trigger Form 8-K Item 1.05, even if each individual occurrence on its own would not rise to the level of materiality."[20]

The definition of "cybersecurity threat" was revised to conform to the cybersecurity incident definition in clarifying that unauthorized occurrences are those "on or conducted through a registrant's information systems." Regarding the definition of "information systems," the SEC inserted "electronic" before "information resources" in the final definition of information systems in response to public comments and to clarify that the definition does not cover hard-copy resources.[21] The SEC declined to define any other terms, including "cybersecurity."[22]

Timing

The above changes became effective September 5, 2023. As noted above, the timing to implement these new disclosure requirements is extremely tight. The following chart summarizes the compliance dates, including applicable transition delays that apply to smaller reporting companies:[23]

	Company That Is Not a Smaller Reporting Company	Smaller Reporting Company
Incident reporting on Item 1.05 of **Form 8-K (and Form 6-K** if otherwise disclosed in a foreign jurisdiction, to any stock exchange, or to security holders)	Beginning on December 18, 2023	Beginning on June 15, 2024
Inline XBRL tagging of Item 1.05 incident reporting on **Form 8-K (and Form 6-K)**	Beginning on December 18, 2024	
S-K 106 disclosure on **Form 10-K (and Form 20-F Item 16K)**	Beginning with annual reports for fiscal years ending on or after December 15, 2023 *For calendar year-end companies this means the Form 10-K filed in 2024 with respect to the year ending December 31, 2023*	
Inline XBRL tagging of S-K 106 disclosure on **Form 10-K (and Form 20-F Item 16K)**	Beginning with annual reports for fiscal years ending on or after December 15, 2024 *For calendar year-end companies this means the Form 10-K filed in 2025 with respect to the year ending December 31, 2024*	

Practical Considerations

For registrants that experience a cyber event, the immediate impact of these new rules will be significant. The rules require focused disclosure controls and procedures, and satisfying the new current reporting obligation hinges on effective communications among many potential stakeholders, including technology teams, external reporting groups, legal teams, management, consultants, and auditors. While many registrants already have in place disclosure controls and procedures relating to cyber events, the new requirements should require, at a minimum, giving those controls and procedures a fresh look. Registrants also should start the education process with the appropriate stakeholders now so that they are able to coordinate efficiently once these new rules take effect. We provide some suggestions to assist in these preparations.

What To Consider When Assessing Materiality

As noted above, registrants must consider both qualitative and quantitative factors when assessing whether the impact of a cybersecurity incident is material. Informed in part by commentary in the adopting release and by our experience helping company's evaluate disclosure obligations under the 2011 Staff Guidance and 2018 Interpretive Guidance, below are some of the factors we believe registrants may generally want to keep in mind when evaluating materiality.

1. Quantitative Considerations
   - Reasonably expected percentage impact on revenue due to lost sales of products or services;
   - Reasonably expected percentage impact on net income due to lost revenues, expenses associated with containing and remediating the incident (including, as applicable, any ransom payment) and other expected expenses (including responding to regulatory and legal proceedings and any voluntary actions to mitigate harm to affected individuals); and
   - Reasonably expected percentage impact on total and current assets of expenses associated with the incident.
2. Qualitative Considerations
   - Relative importance of the systems affected by the incident to the registrant's operations (including how long those systems may be inoperable);
   - Duration of the incident, method of incident detection and readiness of the response to halt the incident;
   - Ability to restore affected systems and the expected integrity of those systems once restored;
   - Nature and scope/magnitude of the information that has been improperly accessed or exfiltrated;
   - Effect of the incident on key systems or information that the registrant considers its "crown jewels";
   - Harm to the registrant's reputation and brand perception;
   - Impact on the registrant's supply chain and operations, including likelihood of consequential harms resulting from delays or other effects of the incident;
   - Impact on relationships with customers (both near-term and over time);
   - Impact on relationships with suppliers and other business partners (both near-term and over time);
   - Effect on the registrant's competitive position relative to its peers (both near-term and over time);
   - Likelihood of regulatory actions by various governmental authorities; and
   - Likelihood of private litigation from individuals whose information has been compromised.
3. Considerations That Typically Will Not Affect the Materiality Analysis
   - Whether the affected system was owned or operated by the registrant or a third-party;
   - Inability to determine the full extent of the incident;

- Ongoing nature of the registrant's internal investigation; and
- Timing of sharing information about the incident with governmental authorities or others.

Controls and Procedures

First and foremost, we recommend that registrants implement cybersecurity disclosure controls and procedures, if they are not already in place. To the extent that registrants have gaps in their existing cybersecurity disclosure controls and procedures, we recommend that they take the time now to review and enhance their overall cybersecurity risk management strategy and governance process. This is a particularly crucial step given the SEC's focus in recent enforcement actions on controls and procedures, as well as the new Regulation S-K Item 106 disclosure requirements.

Incident Response Plans and Procedures

Having an Incident Response Plan (IRP) is one common element of a mature cybersecurity program. As registrants prepare for the new SEC disclosure rules, we recommend that they review and update their processes for responding to cybersecurity events. As part of this review, registrants with an existing IRP and any associated playbooks and procedures should make sure that these materials are updated to ensure that the materiality determination for a cybersecurity incident is not "unreasonably delayed" and give consideration to any definitional differences between material cyber incidents for SEC disclosure purposes and cyber incidents described within the IRP that may be subject to other reporting regimes. Registrants without an existing IRP are well-advised to prepare one.

A comprehensive IRP would include, among other things:

- The goals and scope of the plan;
- A process for identifying, categorizing, escalating, investigating, and remediating potential incidents;
- Defined roles and responsibilities for the incident response team (including clear levels of decisionmaking authority);
- A process for external and internal communications and information sharing;
- A process for SEC disclosure regarding cybersecurity events; and
- A process to review and revise the IRP (as necessary) post-incident to account for lessons learned.

We recommend that in reviewing IRPs, registrants pay particular attention to the communications pathway to ensure that the appropriate decisionmakers are timely alerted to evaluate materiality as required by the new SEC disclosure rules and to consider the need to close the trading window and that there are procedures in place to document both the basis of the materiality analysis as well as the reasonableness of the time it took to make that determination.

Furthermore, IRPs should include a process to evaluate whether it is necessary to request a national security/public safety exception and a process to proceed with the materiality assessment should the request to delay disclosure be denied. We expect that the exception will apply in only very limited circumstances, so registrants should discount the likelihood of its availability. Registrants also should ensure that there are processes in place to address potential inconsistencies in communications over time as the investigation continues to unfold and more information is gleaned after the initial disclosure.

Additionally, as time is of the essence with respect to incident detection, response, and disclosure, registrants may find it helpful to create a communications playbook with pre-approved language for public-facing statements to ensure consistency in communications. Finally, after reviewing an IRP, we recommend that registrants test their revised IRP using a scenario that would require disclosure under the SEC's new rule.

Reviewing Allocation of Oversight Responsibilities & Voluntary Disclosures

Many registrants have their board (or a committee of their board) oversee management's control of cybersecurity risks as part of their overall risk oversight responsibilities. Some registrants also currently

have a separate committee of their board dedicated specifically, in whole or in part, to oversight of cybersecurity matters. Further, many registrants already voluntarily disclose their board's oversight of management's cybersecurity risk practices in their proxy statements, generally as part of the discussion of board committees (and their responsibilities) and/or their board's risk oversight functions.

With new Regulation S-K Item 106 now requiring companies to make certain disclosures in Form 10-Ks about management's role and expertise in assessing and managing cybersecurity related risks, as well as the board's role in overseeing management's control of cybersecurity risk, we recommend that registrants review their current allocation of cybersecurity risk management and oversight and consider whether any changes should be made. Further, we recommend that registrants that have previously provided disclosures in their proxy statements or elsewhere about their cybersecurity risk management practices ensure that such disclosures both adequately reflect their current allocation of cybersecurity risk management and oversight responsibilities between management and the board and are consistent with new cybersecurity risk disclosures to be made in their Form 10-K pursuant to new Regulation S-K Item 106. Additionally, we recommend that registrants confirm that their disclosures do not conflict with any other requirements relating to governance and board reporting to which they may be subject (for example, NYDFS Part 500).

Additional Disclosure Considerations

Disclosures must be carefully drafted and should be the product of careful coordination with the appropriate legal and corporate teams as well as the appropriate security and technical personnel. We recommend that registrants, in addition to evaluating their IRPs, consider whether other privacy and cybersecurity-related rules are applicable and pay close attention to the extent to which compliance obligations with other rules or requirements impact the framing of disclosures. Registrants should expect greater scrutiny of their public filings with respect to cybersecurity moving forward and the information provided may contribute to possible regulatory enforcement or litigation.

Additionally, to the extent that registrants have previously made disclosures related to cybersecurity in their public findings, these companies should consider reviewing their prior risk factor and proxy statement disclosures and assessing the extent to which these need to be enhanced or revised moving forward. Finally, registrants should confirm that the disclosures are, in fact, accurate. For example, to the extent that a registrant makes a representation that a committee of the board meets quarterly to evaluate cybersecurity risk, registrants should expect those quarterly reports to be requested by regulators in connection with investigations of cybersecurity incidents.

For some registrants, there may be additional rules and regulations related to cybersecurity compliance and oversight depending on the nature of the registrant's business, the industry/sector in which they operate, and the types of data that they may hold or access. These additional requirements should be prominent considerations as such registrants draft cyber-related disclosures for purposes of the new SEC disclosure rules.

Select Departures from the Proposing Release

The final rule retreated from a few of the amendments initially proposed. Some of these changes are noted throughout this article. For ease of reference, we have listed noteworthy changes from the proposal:

- Revised Instruction 2 to Item 1.05 of Form 8-K and omitted a proposed Regulation S-K Item 106 amendment, such that certain updated incident disclosures (that is, information that was not known at the time of the initial filing) are to be reported on an amended Form 8-K instead of provided on an ongoing basis in Forms 10-Q and 10-K.[24]

- Added Instruction 4 to Item 1.05 of Form 8-K, which clarifies that a registrant "need not disclose specific or technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede registrant's response or remediation of the incident."[25]
- Removed a proposed requirement to disclose the incident's remediation status, whether it is ongoing, and whether data were compromised.[26]
- Removed a proposed requirement to disclose in a registrant's next periodic report when, to the extent known by management, multiple previously undisclosed, individually immaterial cybersecurity incidents became material in the aggregate.[27]
- Removed a proposed requirement to disclose the frequency of management-board discussions on cybersecurity (though, this may still be disclosed in certain circumstances) under Regulation S-K Item 106(c).[28]
- Removed the proposed amendment to Item 407 of Regulation S-K, which would have required disclosures about cybersecurity expertise, if any, of a registrant's board members.[29]

Notes

1. *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, Release No. 33-11216, 88 Fed. Reg. 51896 (adopted July 26, 2023), *https://www.sec.gov/files/rules/final/2023/33-11216.pdf* [hereinafter Adopting Release].
2. *See* CF Disclosure Guidance: Topic No. 2—Cybersecurity (Oct. 13, 2011), available at *https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm*.
3. *See Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, Release No. 33-10459, 83 Fed. Reg. 8166 (published Feb. 21, 2018).
4. *See Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, Release No. 33-11038, 87 Fed. Reg. 16590 (proposed Mar. 9, 2022), *https://www.sec.gov/files/rules/proposed/2022/33-11038.pdf*.
5. Adopting Release at 10.
6. *Id*. at 11-13.
7. *Id*. at 95-96.
8. *Id*. at 47, 52.
9. *Id*. at 78-79.
10. *Id*. at 31.
11. *See id*. at 37-39 for a discussion of factors that may be relevant to the materiality analysis and the timing of that determination.
12. U.S. Securities and Exchange Commission, *2023 07 06 Open Meeting*, *https://www.youtube.com/watch?v=pWpel8PEy1Y*.
13. Adopting Release, *supra* n.1 at 50-51.
14. *Id*. at 47.
15. *Id*. at 63.
16. *Id*. at 64.
17. *Id*. at 63.
18. *Id*. at 83-85.
19. *Id*. at 69.
20. *Id*. at 76.
21. *Id*.
22. *Id*. at 80-81.
23. *Id*. at 107.
24. *Id*. at 50-52.
25. *Id*. at 30.
26. *Id*.
27. *Id*. at 47, 52.
28. *Id*. at 69. Note, however, that some registrants may, depending on the context, include the frequency in which their board or board committee is informed about cybersecurity risks when describing their processes. *Id*.
29. *Id*. at 83-85.

ESG

European Union Adopts Long-Awaited Mandatory ESG Reporting Standards

By Beth Sasfai, Michael Mencher, Emma Bichet, Jack Eastwood, and Steven Holm

In January 2023, the European Union adopted the Corporate Sustainability Reporting Directive (CSRD), which requires EU and non-EU companies with activities in the European Union to file annual sustainability reports alongside their financial statements. These reports must be prepared in accordance with European Sustainability Reporting Standards (ESRS).

On July 31, 2023, the European Commission adopted the first set of ESRS. The ESRS soon will become law and will apply directly in all 27 EU member states, but not in the United Kingdom. Companies will need to report in compliance with these new ESRS as early as the 2024 reporting period.[1]

The standards are notable for their breadth and granularity, going well beyond the reporting requirements in other mandatory and voluntary environmental, social, and governance (ESG) reporting frameworks. It is clear that companies in scope need to start getting ready to report to these new ESRS now.

The ESRS

The ESRS set out detailed reporting requirements for EU companies in scope of the CSRD, including EU subsidiaries of non-EU companies. The ESRS cover:

1. General reporting principles.
2. A list of mandatory disclosure requirements for EU companies related to the identification and governance of sustainability matters.
3. The 10 ESG topics where disclosure is required, subject to a materiality assessment.

While this is the first set of ESRS, further sets of standards also will be adopted in the near future for specific industry sectors, small and medium-sized enterprises (SMEs) and non-EU parent companies.

Together, the CSRD and ESRS require companies to:

- Perform materiality assessments on each sustainability topic applying the **double materiality principle** to work out which information should be reported. (In line with double materiality, companies must report if sustainability information is material from either a financial or an impact perspective, taking account of people and the environment.)
- Report on the material **impacts, risks and opportunities** (IROs) identified in the company's own operations, those of its group and those of its **upstream and downstream value chain**.
- Provide **metrics and targets** for material sustainability topics and connect these to their financial reports.
- Have their sustainability disclosures **audited by an independent third-party auditor** before they are filed with the relevant authority.

General Requirements

ESRS 1 on "General Requirements" explains the process requirements that apply to all companies reporting under these standards. For example, it

Beth Sasfai, Michael Mencher, Emma Bichet, Jack Eastwood, *and* **Steven Holm** *are attorneys of Cooley LLP.*

explains what is meant by double materiality and reporting boundaries, as well as the extent to which a company must report on its value chains, due diligence expectations, the required quality of quantitative and qualitative data (including the use of estimates), the need for consistency with the company's financial statement disclosure, and the overall report structure.

General Disclosures

ESRS 2 on "General Disclosures" lists all the mandatory disclosures that all in-scope companies must report on, irrespective of materiality. This standard includes disclosures on how sustainability-related performance is integrated into the company's incentive schemes, statements on its due diligence processes and descriptions of the processes used to identify and assess materiality. Disclosures on key performance indicators prescribed by the EU Taxonomy Regulation also are required.

Topical ESRS

Materiality assessments: For the topical ESRS that cover the 10 ESG topics set out in more detail below, a materiality assessment is the starting point for reporting. Companies are required to assess and report on "material" sustainability-related IROs in their value chains under each of the 10 topical standards. If, following the materiality assessment, a given sustainability matter is material from either a financial or impact perspective, the company must disclose against the relevant topical ESRS. The European Commission has been keen to emphasize that reporting on material sustainability matters is not voluntary. The conduct of materiality assessments may require significant advanced planning, including gathering information related to value chain impacts. Companies still will be required to gather sustainability information from their value chains even if, once assessed, they ultimately conclude that the information is not material enough to require reporting.

Where a company has determined that a topical ESRS is not material, it is not required to report information under that standard. However, unlike the other topical ESRS, if a company determines climate-related disclosures (E1) to be immaterial, the company must provide a detailed justification.

Permitted exclusions are very limited, and where a company relies on an exemption, it must disclose this to be the case.

The table below provides an overview of the content for each adopted topical ESRS.

Environmental	
E1 Climate change	■ Disclosures on climate change mitigation, climate change adaptation and energy consumption. ■ Disclosures on climate change mitigation relate to the company's efforts to limit global warming to 1.5°C in line with the Paris Agreement. ■ Disclosures on Scopes 1, 2 and 3 greenhouse gas emissions and transition risks.
E2 Pollution	■ Disclosures on pollution of the air, water, soil, living organisms and food resources, as well as the use of substances of concern and microplastics. ■ This standard covers pollutants generated or used during production processes and those that leave facilities as emissions, products, or as part of products or services.
E3 Water and marine resources	■ Disclosures on consumption, withdrawal and discharge from and into water (including ground and surface water) and marine resources. ■ This standard also requires consideration of the extraction and use of marine resources.
E4 Biodiversity and ecosystems	■ Disclosures covering areas such as the drivers of biodiversity loss, impact on species, and impacts and dependencies on ecosystems.

E5 Circular economy	■ Disclosures on resource inflows, outflows, waste, resource optimization and the risks of the transition to a circular economy. ■ A circular economy is one in which the value of products, materials and other resources in the economy are maintained for as long as possible, enhancing their efficient use in production and consumption, thereby reducing the environmental impact of their use, minimizing waste and the release of hazardous substances at all stages of the product life cycle.
Social	
S1 Own workforce	■ Disclosures on the company's own workforce, including: freedom of association, working conditions, access to equal opportunities and other work-related rights.
S2 Workers in the value chain	■ This standard is similar to ESRS S1 in content but requires consideration of the workers in the company's value chain(s).
S3 Affected communities	■ Disclosures on the impact of a company's own operations and value chain, including: its products and services, impact on indigenous rights, civil rights, and social and economic rights, including water and sanitation, among others.
S4 Consumers and end-users	■ Disclosures on the impacts of a company's products and/or services on consumers and end users, including: access to quality information, privacy and the protection of children. ■ Companies are not required to consider the unlawful use or misuse of products or services.
Governance	
G1 Business conduct	■ Disclosures on anti-corruption and anti-bribery practices, the protection of whistle blowers, political lobbying and the management of relationships with suppliers (including payment practices).

Sector-Specific Standards and Additional Forthcoming Standards

The ESRS outlined above do not represent the entirety of potential disclosure obligations under the CSRD. Sector-specific standards that will apply in addition to the current ESRS are expected to cover sectors such as textiles, information technology, electronics, and pharmaceuticals and biotechnology. These standards would create additional disclosure requirements related to topics of particular materiality for specific industries. Drafts of these standards initially were scheduled for 2023–2024.

Other sets of sustainability standards will be adopted by the European Union in the coming years for SMEs and non-EU parent companies.

Further application guidance also can be expected in the coming months. The European standards body—the European Financial Reporting Advisory Group—is currently developing additional guidance on how companies can perform the double materiality assessment and the extent of value chain information required under the ESRS.

Key Elements for Businesses

Companies in scope of the CSRD should start getting ready for ESRS reporting now, as it may take some time to perform materiality assessments and set up systems to gather the audit-ready data needed for their reports. Key elements for businesses are outlined below.

1. ***Centrality of materiality assessments.*** Companies will need to front-load work in this area to determine the scope of their reporting requirements under each of the topical ESRS. Outside advisers likely will play a key role in helping companies design relevant processes, which must include an analysis of value chains and double materiality, and likely will differ substantively from companies' existing sustainability reporting frameworks or risk management systems.

2. ***Process cannot be neglected.*** The ESRS are very detailed on ***what*** companies should report on and ***how*** they should report. This means that most companies will need to assess whether their existing sustainability diligence and reporting

practices comply with the CSRD, even if they already report on some or all of the areas covered by the topical ESRS. Similar to US Securities and Exchange Commission (SEC) cybersecurity and climate rules, as well as the widely used Task Force on Climate-Related Financial Disclosures (TCFD) and CDP climate disclosure frameworks, the ESRS has a significant focus on disclosures related to the governance of sustainability matters. Companies should be attentive to preparing for the mandatory process and governance disclosures in ESRS 2.

3. ***Importance of climate materiality.*** Perhaps the most notable feature of the adopted ESRS is the move away from proposed mandatory reporting on climate change, including the disclosure of scopes 1, 2, and 3 greenhouse gas emissions. Nonetheless, in practice, we anticipate that most companies will need to report on climate change, given the breadth of the double materiality framework and the need to justify any decision to exclude climate reporting, and have that justification pass audit. At the same time, we are seeing increased investor and customer demands for climate data, meaning, in practice, many companies will be making these disclosures anyway.

4. ***Greater consistency with other ESG reporting frameworks, but gaps remain.*** Although the SEC's final climate rule is not expected until later this year, the ESRS differ from the SEC's current and proposed rules in numerous substantive and methodological areas. Divergences include how the ESRS approach to value chain reporting, the need for impact materiality assessments and the need to report on a broader set of sustainability topics. The ESRS also are broader than just climate disclosures and extend well beyond the current limited SEC requirements related to human capital and governance matters. For US companies already aligning voluntarily with frameworks such as the Global Reporting Initiative, Sustainability Accounting Standards Board or TCFD, the ESRS also contains numerous significant differences in subject matter and methodology.

Similarly, while improvements have been made to better align the ESRS and International Sustainability Standards Board (ISSB) standards—IFRS S1[2] and IFRS S2,[3] published June 2023—companies should not assume that a CSRD-compliant report will automatically meet all the requirements under the ISSB standards, and vice versa. For UK and Singapore companies, this is particularly relevant. On August 2, 2023, the UK government confirmed that the incoming UK Sustainability Disclosure Standards will be based on the ISSB standards.[4]

Conclusion

These new UK sustainability reporting requirements may apply to companies as early as July 2024. A similar proposal has been made in Singapore, where certain companies may be required to comply as early as 2025. The publication of a summary comparing the ESRS to the ISSB standards is expected in the coming months. As a result, we recommend that companies conduct gap assessments of their current voluntary reporting or other regulated disclosures against the ESRS to identify areas where additional work will be required.

Notes

1. *https://ec.europa.eu/finance/docs/level-2-measures/csrd-delegated-act-2023-5303-annex-1_en.pdf.*
2. *https://www.ifrs.org/issued-standards/ifrs-sustainability-standards-navigator/ifrs-s1-general-requirements/.*
3. *https://www.ifrs.org/issued-standards/ifrs-sustainability-standards-navigator/ifrs-s2-climate-related-disclosures/.*
4. *https://www.gov.uk/guidance/uk-sustainability-disclosure-standards.*

DEI

DEI Initiatives Post-*SFFA*: Considerations for Boards and Management

By Martin Lipton, John F. Savarese, Adam J. Shapiro, Erica E. Bonnett, Noah B. Yavitz, and Carmen X. W. Lu

It is no secret that US corporations face vigorous, and often conflicting, demands concerning diversity, equity, and inclusion (DEI) initiatives. Over the past year, DEI initiatives and commitments have come under pressure in the face of macroeconomic headwinds, political scrutiny, and legal challenges. That pressure has only grown following the Supreme Court's recent decision against affirmative action in *SFFA* v. *Harvard*, after which Attorneys General from both red and blue states sent conflicting letters to Fortune 100 companies on what the *SFFA* decision meant for corporate DEI initiatives.[1]

Managing the tension between proponents and opponents of DEI programs and initiatives is particularly complex because of the range of stakeholders involved. Shareholders, employees, customers, suppliers, regulators, stock exchanges and state legislatures are among the groups that have sought to shape the DEI agenda. DEI is no longer only a domestic issue. The European Union's Corporate Sustainability Reporting Directive, which is expected to affect over 3,000 US companies, includes disclosure standards that require firms to assess and disclose workforce and supplier diversity, equity and inclusion policies, practices and metrics to ensure equal treatment and opportunities for all.[2]

Martin Lipton, John F. Savarese, Adam J. Shapiro, Erica E. Bonnett, Noah B. Yavitz, *and* **Carmen X. W. Lu** *are attorneys of Wachtell, Lipton, Rosen & Katz.*

Boards and management seeking to navigate across this rapidly shifting DEI landscape should keep the following principles in mind:

- Directors and officers of public companies in the United States bear fiduciary responsibilities to develop and adopt good-faith policies and strategies designed to maximize the long-term value of the corporation. To that end, boards and management, as part of an informed and deliberate exercise of business judgment, may consider and in turn determine that certain DEI initiatives and strategies advance the company's mission and operational success, by, for example, bringing diverse perspectives to bear on business decision-making and aligning the company's aspirations in this area with those of its workforce, customers, and other constituencies.
- When a DEI policy or strategy is determined, as a matter of business judgment, to further the company's prospects for long-term value maximization, companies should carefully consider how best to communicate the business-grounded rationale for such undertakings and how the company has assessed and sought to balance the competing priorities of its stakeholders. Among the factors to consider include evidence of how DEI initiatives help attract and retain key talent, the impact of DEI strategies on the risk of employment-discrimination claims, how diverse perspectives contribute to better decisionmaking and business outcomes, and how returns from DEI strategies are commensurate with corporate resources used to further such initiatives.
- Corporate policies and initiatives aiming to promote equity and inclusion and eliminate

bias across the workforce and supply chain that were lawful prior to *SFFA* remain lawful after the Court's decision. For example, the latest Supreme Court ruling does not prohibit employers from continuing efforts to reduce bias in hiring and promotion decisions, provide unconscious bias training, conduct outreach to diverse colleges and candidates, include diverse candidates as part of interview slates, establish employee resource groups, include diverse suppliers as part of RFPs, conduct outreach to underserved communities, facilitate mentorship and other pipeline programs to facilitate employee retention, and implement family-friendly and flexible work options.

US Equal Employment Opportunity Commission Chair Charlotte A. Burrows has publicly reiterated that DEI initiatives that were legal prior to *SFFA* remain so.[3]

- Setting DEI goals is not *per se* illegal provided the means by which such objectives are pursued are legally permissible. For example, care needs to be taken to ensure that goals are not accomplished through quotas and other mechanistic tools that utilize race or gender or other protected categories as a "tiebreaker"—or where an individual's race, color, religion, sex, or national origin is otherwise explicitly factored into employment decisionmaking, because such practices can violate Title VII of the Civil Rights Act and other antidiscrimination laws that prohibit the use of such protected categories in rendering employment decisions. Employment decisions, including hiring, compensation and promotion, should instead focus on permissible considerations such as the challenges an individual has overcome, the contributions the individual has made to the company's success, and the perspectives and background that an individual may bring to bear on the company's long-term business success.
- While legal scrutiny over corporate DEI initiatives is likely to continue to increase, along with claims of reverse discrimination, the burden of proof borne by plaintiffs has not changed. Plaintiffs seeking to prove discrimination under Title VII will still need to prove that they suffered an "adverse employment action" that was motivated by their race, color, religion, sex or national origin.

  Companies should continue, as they have done in the past, to maintain practices and procedures that demonstrate compliance with the law. Directors and senior management, for their part, should reinforce the importance of strict adherence to these standards.

The Supreme Court's decision in *SFFA* has not altered the fiduciary obligations of employers nor has it redrawn the permissible legal contours of DEI initiatives. We nonetheless expect companies to continue facing heightened scrutiny from all sides over why and how they go about identifying, evaluating and implementing DEI policies and goals. For these reasons, we encourage all companies to periodically review and assess their DEI strategies and commitments to ensure they align with broader business purposes and are being implemented in a manner that promotes equity and inclusion for all.

Notes

1. For example, *see https://www.tn.gov/content/dam/tn/attorneygeneral/documents/pr/2023/pr23-27-letter.pdf* and *https://illinoisattorneygeneral.gov/News-Room/Current-News/Fortune%20100%20Letter%20-%20FINAL.pdf*.
2. *See https://www.efrag.org/Assets/Download?assetUrl=%2Fsites%2Fwebpublishing%2FSiteAssets%2F13%2520Draft%2520ESRS%2520S1%2520Own%2520workforce%2520November%25202022.pdf* and *https://www.efrag.org/Assets/Download?assetUrl=%2Fsites%2Fwebpublishing%2FSiteAssets%2F14%2520Draft%2520ESRS%2520S2%2520Workers%2520in%2520the%2520value%2520chain%2520November%25202022.pdf*.
3. *https://www.eeoc.gov/newsroom/statement-eeoc-chair-charlotte-burrows-supreme-court-ruling-college-affirmative-action*.

REGULATION A+

Regulation A+: Recent SEC Enforcement Proceedings and Comment Letter Trends

By David H. Roberts and Mark Schonberger

In March 2015, the Securities and Exchange Commission (SEC) adopted amendments to Regulation A, which expanded the Regulation A exemption from the Securities Act of 1933 (the Securities Act) registration for public offerings up to $50 million in any 12-month period (also known as Regulation A+ or Reg A+), as mandated by Title IV of the Jumpstart Our Business Startups Act. The Reg A+ offering limit was raised by the SEC to $75 million in any 12-month period in November 2020.

Offerings under Reg A+ also are subject to reduced disclosure requirements and less onerous ongoing reporting requirements as compared to the full Securities Exchange Act of 1934 (the Exchange Act) requirements. Reg A+ was adopted to facilitate capital raising by smaller companies while still providing investor protection. In the SEC's Report to Congress on Regulation A/Regulation D Performance, dated August 2020, the SEC noted that from June 19, 2015, through December 31, 2019, the SEC qualified 382 Regulation A offerings seeking to raise approximately $9.1 billion.

Although Reg A+ was adopted to facilitate capital raising, the SEC's Staff (the Staff) has been reminding Reg A+ issuers through enforcement proceedings and comment letters that they still must comply with SEC rules and regulations for these offerings. The SEC's Division of Enforcement (Enforcement Division) has recently settled a number of proceedings with Reg A+ issuers, and the SEC's Division of Corporation Finance (Corporation Finance) has issued comment letters to existing Reg A+ issuers on various topics. This article provides details on the areas of focus in the Enforcement Division's proceedings and Corporation Finance's comment letters.

David H. Roberts *and* **Mark Schonberger** *are partners of Goodwin Procter LLP.* *The authors wish to acknowledge* **Martin Green** *for his assistance with this article.*

Enforcement Proceedings

On May 16, 2023, the Enforcement Division settled enforcement proceedings with 10 Reg A+ issuers with alleged offering infractions spanning several years. The fines ranged from $5,000 to $90,000, and the issuers were ordered to cease and desist from committing or causing any violations and any future violations of Section 5 of the Securities Act. The Enforcement Division proceedings pertaining to Reg A+ offerings fell into the following five categories:

1. *Increased Offering Size*—increasing the number of securities being sold without filing new offering statements (Form 1-As) or post-qualification amendments (PQAs) to obtain qualification for the modified offerings.
2. *Change in Offering Price*—revising the offering price by more than 20 percent without filing new Form 1-As or PQAs to obtain qualification for the modified offerings.
3. *At-the-Market Offering*—conducting an at-the-market offering.
4. *Delayed Offering*—conducting a delayed offering.
5. *Annual Updating*—failure to update financial statements at least annually through a PQA.

Increasing the Number of Securities Being Sold

Seven out of the ten Enforcement Division proceedings pertained to Reg A+ issuers increasing the

number of securities being sold without filing a new Form 1-A or PQA to obtain qualification for the modified offerings. In each case, the issuer attempted to increase the number of securities being offered in connection with an ongoing Reg A+ offering by filing an offering circular supplement. Under the SEC's rules, to offer additional securities, a Reg A+ issuer must add those securities by filing a new Form 1-A or PQA, which the SEC must then qualify.

Revising the Offering Price

Six out of the ten Enforcement Division proceedings pertained to Reg A+ issuers revising the offering price by more than 20 percent without filing new Form 1-As or PQAs to obtain qualification for the modified offerings.

The SEC noted in its orders that an issuer is not permitted to use an offering circular supplement to fundamentally change the information set forth in an offering statement. Instead, such changes require a new Form 1-A or PQAs, each of which must be qualified by the SEC. A fundamental change may be present when an issuer changes the price of securities offered under Reg A+. Although not explicitly noted in the Enforcement Division orders, the SEC has historically held that a change in offering price greater than 20% would be considered a fundamental change.

Conducting an At-the-Market Offering

Two out of the ten Enforcement Division proceedings pertained to Reg A+ issuers conducting an at-the-market offering.

An issuer is not permitted to conduct an at-the-market offering under Reg A+. An at-the-market offering is defined in Reg A+ as an "offering of equity securities into an existing trading market for outstanding shares of the same class at other than a fixed price." The issuers failed to comply with Reg A+ by changing the price of the offering multiple times.

Conducting a Delayed Offering

One out of the ten Enforcement Division proceedings pertained to a Reg A+ issuer conducting a delayed offering. A delayed offering is an offering that does not commence within two calendar days and is not permitted under Reg A+.

Failure to Update Financial Statements

Three out of the ten Enforcement Division proceedings pertained to Reg A+ issuers failing to update financial statements at least annually through a PQA. To conduct an ongoing Reg A+ offering, an issuer is required to file a PQA at least every 12 months after the qualification date to include the financial statements that would be required by Form 1-A.

Staff Comment Letters

In addition to the Enforcement Division proceedings noted above, Corporation Finance has also been focusing on Reg A+ issuers. We reviewed all comment letters issued to existing Reg A+ issuers (that is, not in connection with qualification of their initial offering) in the last 12 months. These comments letters were in connection with the Staff's review of PQAs and Form 1-As filed other than in connection with initial offerings.

We found that the Staff sought additional disclosure or explanation concerning:

- *At-the-Market and Delayed Offerings*—whether an offering is being made at a fixed price or is a delayed offering.
- *Marketing Materials*—compliance of disclosure posted on issuer websites, on social media accounts, and in advertisements.
- *Updating for New Financials*—updates to qualified Form 1-As related to interim or annual financial statements and auditor consents.
- *Series Offering Disclosure*—for issuers that are series LLCs, disclosure related to open and closed series offerings.

Fixed Price and Delayed Offerings

Similar to the Enforcement Division proceedings noted above, a number of comments focused on whether Reg A+ issuers were conducting delayed offerings or offerings at other than a fixed price. As

noted above, delayed offerings and at-the-market offerings are not permitted under Reg A+.

One issuer argued that the offering was not an at-the-market offering because there was no existing trading market for the issuer's securities. It is unclear if the Staff accepted this argument or one of the other arguments made by the issuer that the offering was not an at-the-market offering. We agree that an offering should not be considered an at-the-market offering if there is no "existing trading market."

Compliance of Disclosure Posted on Issuer Websites, in Social Media Postings and in Advertisements

In a number of instances, the Staff indicated that they reviewed issuer websites, social media postings, and advertisements in connection with the Staff's review of issuer filings. In connection with that review, the Staff had the following comments:

- Whether an issuer's online advertising complied with Rule 251(d) or Rule 255(b) of Reg A+.[1] The Staff also asked that all testing-the-water materials, including any advertisements posted on third-party websites and an issuer's Twitter account, be filed with the SEC and for the issuer to explain how it complied with Rule 255(b) of Reg A+.
- Whether certain information posted on an issuer's Twitter account also should have been posted on a Form 1-U.
- The Staff requested that the issuer make a number of corrections and updates to information posted on the issuer's website.

Updates to Qualified Form 1 As Related to Interim or Annual Financial Statements and Auditor Consent

In a number of instances, the Staff asked Reg A+ issuers to update their financial statements with the most recent interim or annual financial information. For example, in one instance, the Staff asked an issuer (that is registered under the Exchange Act) to update its Form 1-A to include the interim financial statements and related information from its Form 10-Q. In a number of instances, the Staff also asked issuers to file updated auditor consents with their PQAs. It should be noted that under Rule 252(f), an auditor consent needs to be filed with a PQA only if the previously filed audited financial statements have been amended.

Disclosure Related to Open and Closed Series Offerings

In a few instances, the Staff was focused on disclosure pertaining to the offering of different series for issuers that are series LLCs. In one instance, the Staff noted that the offering table on the cover page of the offering circular should include only ongoing series offerings and not closed offerings. In another instance, the Staff noted that an issuer should update its master series table to include open and closed offerings, not just open offerings.

Next Steps

Given the noted enforcement proceedings and comment letters, existing Reg A+ issuers should keep in mind that although Reg A+ was meant to be less onerous than seeking registration, they still must comply with the SEC's rules and regulations for these offerings, and they should consider how these enforcement actions and comment letters may impact their offerings and disclosures going forward. As always, the Goodwin team is available to answer any questions you have and assist with compliance.

Note

1. Rule 251(d) states that offers may be made after an offering statement has been qualified, but any written offers must be accompanied with or preceded by the most recent offering circular filed with the SEC for such offering. Rule 255(d) pertains to the solicitation of interests and other communications before the qualification of an offering statement.

DISCLOSURE PRACTICES

Companies Should Exercise Caution in Describing Pending Litigation as "Without Merit"

By Charlie Gili, Adorys Velazquez, Travis J. Wofford, Richard B. Harper, and Quentin W. Wiest

Public companies should be cautious when describing litigation as "without merit" or meritless if they have reason to know otherwise. It could form the basis of a disclosure claim under the securities laws. A securities fraud putative class action suit in federal court against Pegasystems Inc. (Pega) recently survived a motion to dismiss where: (1) Pega was sued for trade secret misappropriation; (2) Pega's CEO publicly claimed the trade secret lawsuit was "without merit;" (3) thereafter, the trade secret lawsuit returned a judgment against Pega for over $2 billion in damages; and (4) sufficient facts were alleged that Pega's CEO personally participated in the trade secret misappropriation.[1]

As the court in the securities fraud litigation noted, "An issuer may legitimately oppose a claim against it, even when it possesses subjective knowledge that the facts underlying the complaint are true. When it decides to do so, however, it must do so with exceptional care, so as not to mislead investors…. An issuer may not … make misleading substantive declarations regarding its beliefs about the merits of the litigation."

Background

In May 2020, Appian Corp. (Appian) sued Pega for, among other things, trade secret misappropriation, alleging a corporate espionage campaign led by Pega's CEO. Appian initially sought damages of $90 million (less than 10 percent of Pega's then reported current assets).[2]

In subsequent public filings, Pega included only generic disclosure that, "[w]e have received, and may in the future receive, notices that claim we have misappropriated … [other's] intellectual property rights."

In February 2022, Appian filed to increase its claim to approximately $3 billion (four times Pega's then-current assets and roughly three times its prior year's annual revenue). Three business days later, Pega filed its Annual Report on Form 10-K that included new disclosures about the litigation, as well as a statement that the lawsuit was "without merit" and that "any alleged damages claimed by Appian are not supported by the necessary legal standard…." The following day, Pega's stock dropped approximately 16%.

In May 2022, a unanimous jury verdict awarded Appian over $2 billion in damages. Pega's share price dropped approximately 28 percent in the following two days. Shortly thereafter, investors brought a securities fraud class action against Pega, its CEO and its CFO alleging that the defendants, despite knowingly engaging in the conduct underlying Appian's civil suit, had falsely assured investors that Appian's claims were meritless. Pega moved to dismiss for failure to state a claim, alleging that the Plaintiff had not sufficiently pled facts establishing, among other things, a strong inference of scienter and that the challenged statements were false or misleading.

Holding

Based on the factual allegations made by the investors, the court denied Pega's motion to dismiss, except with respect to the CFO.

Charlie Gili, Adorys Velazquez, Travis J. Wofford, Richard B. Harper, *and* **Quentin W. Wiest** *are attorneys of Baker Botts LLP.*

The allegations of the CEO's personal involvement in the misconduct underlying the trade secret litigation provided support for the scienter requirement in the securities fraud claim. The court noted that "[the CEO] knew or was reckless in not knowing that . . . his assurance that Appian's claims were "without merit" posed a substantial danger to mislead investors." The court further noted that the CEO's assurances were false and misleading under the Private Securities Litigation Reform Act (PSLRA), as well as causally connected to the drop in value of Pega stock that had occurred in February and May of 2022. The court explained that a reasonable investor would have expected that the CEO's statement would have fairly aligned with the information in his possession at that time, when in fact the CEO's statement did not, as he allegedly had direct involvement in the conspiracy.

Notably, the court stated that "a reasonable investor could justifiably have understood the CEO's message that Appian's claims were 'without merit' as a denial of the facts underlying Appian's claims—as opposed to a mere statement that Pega had legal defenses against those claims."

Takeaway

Public companies who routinely claim that litigation is "without merit" should pay attention to this case. While the company is appealing the ruling, it still serves as a good reminder to avoid boilerplate litigation contingency disclosures.

In particular, companies must be cautious where statements by executives regarding ongoing litigation may conflict with the underlying facts, litigation status or written disclosures. Where the underlying facts and litigation outcome are not known for certain, statements investors may perceive as nullifications of risk (such as claims the litigation is "without merit") should not be made without thoughtful consideration.

Still, the court was clear that companies need not confess to wrongdoing. Instead, companies should consider statements, if true, such as: we plan to vigorously defend ourselves; we have substantial defenses; we intend to pursue all available administrative and judicial remedies necessary to resolve these matters; we intend to dispute these allegations; and we are confident in our ability to prevail on the merits—each of which may have the benefit of still being true even where the underlying allegations may be true. Additionally, qualifications, cautionary language and appropriate PSLRA disclaimers can be significantly helpful.

This ruling does not replace our prior guidance as to how companies should approach litigation contingency disclosures.[3]

Also, the result in this case may have been different had the alleged facts not met the *scienter* requirement. In particular, the facts supported the inference that the executives asserting the trade secret claim was "without merit" were the same individuals perpetrating the trade secret violations.

Side note: Another noteworthy piece of this securities fraud class action involves a statement in Pega's Code of Conduct that it would "[n]ever use illegal or questionable means to acquire a competitor's trade secrets"—the exact misconduct allegedly perpetrated by the CEO in this case. The court held that the Code of Conduct statement was not merely aspirational but was an actionable commitment to investors to avoid "a specific course of conduct." This is a good reminder that companies should routinely review their corporate governance policies to ensure they are complying with the policies and not merely treating the policies as a statement of the company's goals and aspirations. Investors and courts will expect companies to adhere to the commitments made in corporate policies.

Notes

1. *https://ia801506.us.archive.org/16/items/gov.uscourts.mad.246980/gov.uscourts.mad.246980.92.0.pdf.*
2. Regulation S-K Item 103(b) provides public companies with a safe harbor from the requirement to disclose material pending litigation if the claim for damages is less than 10 percent of the company's consolidated current assets.
3. *https://www.bakerbotts.com/thought-leadership/publications/2019/october/mylan-settlement-shines-a-light-on-disclosure.*

GENERATIVE AI

Generative Artificial Intelligence and Boards: Cautions and Considerations

By Lawrence A. Cunningham, Arvin Maskin, and James B. Carlson

Generative AI (that is, AI creating original content using machine learning and neural networks) has captivated people everywhere, eliciting a range of responses; from doomsday warnings of machines rendering humans extinct to rosy dreams where machines possess magical properties. In corporate boardrooms, however, a more sober conversation is occurring. It seeks a practical understanding of how boards might evaluate this powerful, but error-prone, new tool, and comes with both cautions about its downsides and considerations for potential upsides.

Companies are racing to harness the benefits of generative AI while trying to develop policies to protect against reputational and regulatory risks and that create a clearer role for boards of directors. The generative AI industry continues to debate and refine its offerings as well, which have become more effective with each subsequent iteration of generative AI. Policymakers are weighing in with a flurry of regulatory initiatives and recommendations in the face of concern about the ethical implications and other risks of widespread adoption of this new tool.

In this article, we offer corporate boards insight about generative AI along with practical cautions, noting both its perils and promise. We also touch on current regulatory initiatives and legal issues for directors.

Lawrence A. Cunningham, **Arvin Maskin**, *and* **James B. Carlson** *are attorneys of Mayer Brown.*

Regulatory Initiatives in the United States and Across the Globe

Generative AI has been the subject of multiple regulatory and political initiatives worldwide, focused on potential risks in the use of AI and achieving a balance between innovation, accountability, and transparency. While there is not a comprehensive legal framework for the regulation and oversight of AI in the United States, legislative efforts around AI indicate an increasing drive for Washington to assume a significant position in the regulation of AI. For example, in the United States:

- The White House issued a fact sheet outlining a series of executive actions addressing generative AI, including a blueprint for a generative AI "bill of rights," and its Office of Science and Technology issued a request for information on oversight of generative AI systems.[1]
- The Department of Commerce's National Institute of Standards and Technology (NIST) released a framework for voluntary use and to promote trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems, including notably suggesting that companies "establish policies that define the artificial intelligence risk management roles and responsibilities . . . including board of directors . . ."[2]
- The Federal Trade Commission (FTC), the Justice Department's Civil Rights Division and the Equal Employment Opportunity Commission issued a joint statement focusing on generative AI's risks of bias.[3]
- The FTC has also separately warned that certain generative AI usage could violate federal laws the FTC enforces[4]

- Widely-publicized hearings on generative AI were recently held before the Senate Judiciary Committee and the House Judiciary Subcommittee on the Courts, Intellectual Property and the Internet and Sub Committee on Cybersecurity, Information Technology and Innovation, providing an opportunity to discuss trends, implications, and risks associated with AI and potential regulatory and oversight frameworks.[5]
- State and local government initiatives are underway nationwide, including in California, Colorado, Illinois, Vermont, Washington, and New York City.

Outside the United States, wide-ranging regulatory initiatives are being considered, including:

- The European Union's proposed AI Act and AI Liability Directive specifying obligations for provider of generative AI models.[6]
- The United Kingdom government's AI regulation policy paper and AI white paper.[7]
- Brazil's proposed Legal Framework for Artificial Intelligence.[8]
- Canada's proposed Artificial Intelligence and Data Act.
- China's Cyberspace Administration of the proposed Administrative Measures for Generative Artificial Intelligence Services.[9]

This intense global focus on the potential uses and misuses—and related responsibilities and obligations—point towards the need for corporate boards to establish policies and processes to address generative AI risk management. At the same time they need to evaluate how generative AI may be properly used to gain strategic and competitive advantages.

Evolving Scope

Generative AI produces content based on natural language inputs, such as memos, queries, or prompts. Output varies in quality, accuracy, and objectivity.

The more widely-available popular generative AI tools tend to be designed for general audiences. At this point, many lack the technical specifications and precision that companies or professional groups will find desirable from the relevant databases and guardrails to depth of analysis, tone, or diction, and references to authority.

Some industries are likely to be touched by the technology in more obvious ways than others—publishers and software firms possibly more at the moment than building contractors or mining companies for instance. Oversight will correspondingly vary as will required training, supervision, and restrictions or permissible uses.

Many companies are developing policies and procedures specifically applicable to the use of generative AI by officers and employees. They are updating their corporate policies to address concerns about potential risks and harms in the context of generative AI, such as bias/discrimination, confidentiality, consumer protection, cybersecurity, data security, privacy, quality control, and trade secrets.

Director Duties and Recommended Precautions

Generative AI does not change the bedrock fiduciary duties of corporate directors and using or otherwise incorporating AI into board decisionmaking is certainly no substitute for the traditional means of discharging them. For example, directors must, consistent with their duty of care, act in an informed manner, with requisite care, and in what they, in good faith, believe to be the best interests of the corporation and its shareholders. They must act loyally, including by protecting the confidentiality of corporate information.

If generative AI evolves into a tool that poses challenges to corporate policy or effectiveness or creates material risk, it is reasonable to assume that related oversight function would fall within the fiduciary duties of corporate boards. That would require the board to exercise good faith and act with reasonable care to attempt to assure that management maintains appropriate systems of control over generative AI.

For public companies using generative AI in financial reporting and securities filings, boards

may need to confirm with management that the company appropriately uses generative AI's capabilities in connection with its internal control over financial reporting as well as disclosure controls and procedures.

As generative AI tools proliferate and are incorporated into search and data products already in wide use, directors should consider (1) the degree to which information they receive from management, auditors, consultants, or others may have been produced using generative AI, and (2) whether they can and should use generative AI tools as an opportunity to support their duties and activities as directors. For both purposes, directors must be mindful, like company officers and employees, of risks associated with the company's use and reliance on generative AI. Three of the key considerations are:

First, generative AI are machines, not people. They have no knowledge, expertise, experience, or qualifications—in any field whatsoever, not least corporate governance or business administration. Unlike directors, generative AI owes no fiduciary duties and faces no liability for breach.

Second, generative AI results may be inaccurate, incomplete, or biased (with bogus AI information or output commonly called "hallucinations"). Generative AI can be a valuable tool to generate ideas, provide generally available factual information, spot issues, and create lists. But, at least at present, there are limits on these tools' capabilities. Accordingly, outputs must be scrutinized and tested for trustworthiness, that is, for things such as accuracy, completeness, lack of bias, and explainability (that is, explain how and why AI made a particular recommendation, predication, or decision). Only then should the output be drawn on to incorporate into the activity, discussion, or material of interest.

Third, generative AI processes and retains user interactions as training data, which is intended to improve the quality of its output in future versions, but also implicates privacy and cybersecurity risks and considerations, including the unintended disclosure of confidential information and other data. Corporate directors must therefore take care to avoid generative AI being used in ways that could compromise such confidentiality or create legal exposure.

For example, in the case of confidential or sensitive company information, it is possible that data or document input and output might leak and be incorporated into the wider generative AI model, exposing it to being machine read, trained by, or synthesized into the generative AI models. Accordingly, directors should consider some practical self-limitations, whether or not formalized in corporate policies. For example:

- Not mentioning the company name or other company specific or identifying information in inputs or chats with generative AI.
- Not mentioning any non-public or proprietary information or specific individual names or data in inputs or chats with generative AI.
- Reviewing generative AI output for accuracy and completeness and not simply passing on generative AI output without a thorough review and modifications as necessary.
- Using generative AI output internally and not projecting publicly.
- Identifying, when appropriate, the generative AI output component of any product that involved the use of generative AI.

Of course, this practical guidance for directors may evolve as market practices and company generative AI policies evolve.

For now, in the case of companies that have not done so, boards may want to ask management for a high-level initial report on generative AI and discuss the subject with management, preferably with there being a management point-person for AI oversight, usage, and risk management. The goal would be to assess the extent to which generative AI tools create opportunities—competitive, innovative, or strategic—and/or present risks, whether operationally disruptive, compliance, or financial.

To explore these possibilities, a board might begin by asking management to put the topic on an upcoming board meeting agenda and receive both management's views and perspectives from outside advisors. As part of the process, directors could learn

about generative AI by posing a series of questions to generative AI asking about these issues, consistent with the foregoing common-sense precautions, which may add to the framework for discussion.

In the case of US companies that have made significant—or "mission-critical" investments in AI—boards should consider being able to demonstrate board-level oversight of AI risks. This is particularly important due to potential claims based on standards from the *Caremark* case, which involve directors' failure to oversee corporate compliance risks. While bringing *Caremark* standard cases has traditionally not been easy, the ability of some recent claims to survive motions to dismiss highlight the ongoing significance of this claim for directors responsible for overseeing critical company compliance operations. Therefore, even if a company is not in breach of its regulatory obligations, directors could still face legal claims if they were not sufficiently attentive to important "mission-critical" risks at the board level.

As such and without detracting from the suggestions above, for companies where AI is associated with mission-critical regulatory compliance/safety risk, boards might want to consider: (1) showing board-level responsibility for managing AI risk (whether at the level of the full board or existing or new committees), including AI matters being a regular board agenda item and shown as having been considered in board minutes; (2) the need for select board member AI expertise or training (using external consultants or advisors as appropriate); (3) a designated senior management person with primary AI oversight and risk responsibility; (4) relevant directors' familiarity with company-critical AI risks and availability/allocation of resources to address AI risk; (5) regular updates/reports to the board by management of significant AI incidents or investigations; and (6) proper systems to manage and monitor compliance/risk management, including formal and functioning policies and procedures (covering key areas like incident response, whistleblower process, and AI-vendor risk) and training.

Boards should use these management discussions and reports to help to determine the appropriate frequency and level of board engagement and oversight. This will range from board-only periodic reviews to more regular discussions, including involving one or more board committees.

Notes

1. *https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/04/fact-sheet-biden-harris-administration-announces-new-actions-to-promote-responsible-ai-innovation-that-protects-americans-rights-and-safety/.*
2. *https://www.nist.gov/itl/ai-risk-management-framework.*
3. *https://www.mayerbrown.com/en/perspectives-events/publications/2023/04/us-ftc-doj-eeoc-and-cfpb-release-joint-statement-on-ai-discrimination-and-bias.*
4. *https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems.*
5. *https://www.mayerbrown.com/en/perspectives-events/publications/2023/05/ai-governance--specific-takeaways-for-companies-regarding-the-us-senate-judiciary-hearings.*
6. *https://www.mayerbrown.com/en/perspectives-events/blogs/2022/10/eu-commission-proposes-new-liability-rules-on-products-and-ai.*
7. *https://www.mayerbrown.com/en/perspectives-events/publications/2022/08/uk-government-proposes-a-new-approach-to-regulating-artificial-intelligence-ai.*
8. *https://www.mayerbrown.com/en/perspectives-events/publications/2021/10/brazil-artificial-intelligence-bill-approved-by-chamber-of-deputies.*
9. *https://www.mayerbrown.com/en/perspectives-events/publications/2023/06/gen-ai-china-proposes-draft-measures-for-regulating-generative-artificial-intelligence.*