Cahill

December 20, 2023

New SEC Cyber Incident Disclosure Requirements Take Effect

Public companies face significant challenges and uncertainties under the new reporting requirements that took effect December 18, 2023. On July 26, 2023, the U.S. Securities and Exchange Commission ("SEC") adopted much-anticipated cybersecurity rules that apply to U.S. SEC reporting companies as well as most foreign private issuers. In adopting the final rules, the SEC noted the rising prevalence and gravity of cybersecurity threats and incidents, and investors' need for more timely, reliable and uniform disclosures.[1] The SEC also cited the economic costs resulting from cybersecurity incidents, and increasing reliance on electronic systems that are susceptible to cybersecurity breaches and unknown vulnerabilities. Under the new rules, reporting companies must have, among other things, board and management-level governance structures, controls and procedures to manage cybersecurity risks, and should a material cybersecurity attack be detected, the rules require disclosure of the incident.

Annual reporting requirements start for fiscal years ending on or after December 15, 2023, although for certain smaller companies the effective date will be June 15, 2024. Compliance with the new rules may require significant time to prepare the new disclosures, and companies may be required to implement new compliance processes as well.

Some registrants have already begun disclosing notable cybersecurity incidents in recent disclosures, providing an early look at efforts to address the new requirements in the context of real life incidents. Most notably, two recent disclosures have resulted from cybersecurity attacks on two casinos, MGM and Caesars, reportedly by the hacker group Scattered Spider. Although the two incidents appear to have been carried out independently of each other, the similarities between the two cyberattacks and their close proximity in time offer useful insights into the application of the new rules in practice. The two hacks also serve to illustrate some advantages and disadvantages of the breach response taken by each of the two companies.

The New Rules

The new rules include several broad definitions which may impact similar and overlapping definitions used in other cybersecurity regulations, and which have yet to be interpreted by the SEC:

- A "cybersecurity incident" is an unauthorized occurrence, or a series of related unauthorized occurrences,[2] 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.

---

[1] *See* Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, [Release Nos. 33-11216; 34-97989; File No. S7-09-22] (July 26, 2023).

[2] An element of the proposed rules that would have required companies to aggregate individually immaterial events in order to determine whether a cybersecurity event has taken place was eliminated in the final rules in favor of the final definition's inclusion

- A "cybersecurity threat" is any potential unauthorized occurrence on or conducted through a registrant's information systems that may result in adverse effects on the confidentiality, integrity or availability of a registrant's information systems or any information residing therein.
- "Information systems" are electronic information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of the registrant's information to maintain or support the registrant's operations.

New Item 1.05 of Form 8-K[3] requires disclosure of material cybersecurity incidents within four business days of the company's determination that the incident is material. More specifically, Item 1.05 states: "If the registrant experiences a cybersecurity incident that is determined by the registrant to be material, describe 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."[4] In addition, disclosures under Item 1.05 must be updated or amended with any subsequently determined information that was required by Item 1.05 but not available at the time of the original filing within four business days of its determination, "without unreasonable delay." The trigger for the four business day incident response is a determination of materiality—that is, a company would be required to report the cybersecurity incident four days after determining its materiality, rather than within four days following discovery of the incident itself. A registrant may delay filing if the U.S. Attorney General determines such disclosure would pose a substantial risk to national security or public safety.[5]

Assessing materiality is by no means an exact science, and companies may consider qualitative factors alongside quantitative factors in determining the materiality of a cybersecurity incident. Because it is the determination of materiality that triggers the disclosure requirement, companies should take care to document and support any determinations made. The SEC has also noted that whether an incident is material is not contingent on where the relevant electronic systems reside or who owns them. Under the new rules, materiality must be determined "without unreasonable delay."[6]

As guidance to registrants, the SEC has noted that information regarding the incident need not be complete for disclosure to be required if a company has sufficient information to determine the incident was material, such as when the incident impacts key systems and information, or involves unauthorized access to or exfiltration of large quantities of particularly important data. In these instances, a materiality determination should not be unreasonably delayed while the registrant awaits more detailed information if, as a result, the registrant would fail to meet its disclosure obligations in a timely manner. Examples of unreasonable delay include deferring committee meetings for

---

of a "series of unrelated unauthorized occurrences." *See*, Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents, Release No. 34-97142 (March 15, 2023). That being said, the adopting release emphasizes that the term "cybersecurity incident" should be "construed broadly."

[3] The new rules require comparable disclosures by foreign private issuers on Form 6-K for material cybersecurity incidents.

[4] In the final rule, the SEC streamlined Item 1.05 from the originally proposed version to focus the disclosure primarily on the impacts of a material cybersecurity incident, as opposed to requiring underlying details of the incident itself.

[5] The SEC recently added several Q&As in the Exchange Act Form 8-K Compliance and Disclosure Interpretations related to the delay in filing for the Attorney General determination. These are available at https://www.sec.gov/divisions/corpfin/guidance/8-kinterp.htm.

[6] Under the proposed rules, materiality was to be determined "as soon as reasonably practicable."

the responsible committee, or revising existing incident response policies and procedures to support a delayed materiality determination of an ongoing cybersecurity event.

Under the new rules, registrants must describe their processes, if any, for the assessment, identification, and management of material risks from cybersecurity threats, and describe whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations, or financial condition.[7] The enumerated elements that a registrant should address, as applicable, include the following:

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

Under new Regulation S-K Item 106(a), registrants must also implement governance and reporting requirements that:

- Describe the board's oversight of risks from cybersecurity threats including, if applicable, identifying any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describing the processes by which the board or such committee is informed about such risks.
  - According to the adopting release, the SEC did not include a materiality qualifier here because if a board of directors decides to oversee a particular risk, the fact of such oversight being undertaken by the board is likely material to investors.
- Describe management's role in assessing and managing material risks from cybersecurity threats.
  - The adopting release notes that the SEC modified this requirement to include a materiality qualifier because management oversees many matters, and its oversight of immaterial matters is likely not material to investors.

Item 106(c)(2) of Regulation S-K directs registrants to consider disclosing the following as part of a description of management's role in assessing and managing the registrant's material risks from cybersecurity threats:

- Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise;

[7] The increased SEC focus on cyber disclosures generally is also reflected in the recent complaint against the information technology firm SolarWinds, which highlights several areas of public disclosures in which the company allegedly made multiple materially false and misleading statements and omissions to conceal the company's poor cybersecurity practices and downplay its software vulnerabilities. *See*, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown* (United States District Court for the Southern District of New York) 1:23-cv-09518.

- The processes by which such persons or committees are informed about 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 a committee or subcommittee of the board.

However, Instruction 4 to Item 1.05 of Form 8-K provides 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 the registrant's response or remediation of the incident."

MGM and Caesars File SEC Disclosures on Cybersecurity Incidents

The recent cybersecurity attacks at MGM Resorts and Caesars Entertainment and the resulting Form 8-K disclosures provide some insight into what issues the new rules may raise when applied. The companies' recent cyberattack disclosures and differing responses also illustrate some of the challenges and uncertainties registrants will face when they become the victim of a cyberattack under the new rules.

Occurring within days of one another, both cybersecurity breaches occurred by tricking a help desk agent via social engineering, and both were reportedly the work of the same cybercriminals. As a result of the breach, each casino lost copies of their loyalty program database, with lists of social security and driver license numbers for a significant number of customers.

Caesars filed a Form 8-K with the SEC on September 14, 2023. Its disclosure, made under Item 8.01 (Other Events) of Form 8-K, included various details about the nature and scope of the cyberattack, including the use of social engineering on their outsourced IT vendor to carry out the attack.[8] However, the disclosure noted that the incident was not discovered until September 7, 2023 and also noted that the company had paid an unspecified ransom to the hackers.[9] In contrast, MGM made its disclosure slightly more quickly, furnishing its Form 8-K on September 13, 2023, within four business days of being attacked. The MGM disclosure, made under Item 7.01 (Regulation FD disclosure) of Form 8-K, included comparatively little information about the attack, however, and according to a subsequently furnished October 5, 2023 Form 8-K, also under Item 7.01 (Regulation FD disclosure), MGM has reportedly not paid any ransom. [10]

The differences in timing and degree of detail between the two responses illustrate some of the trade-offs that impact a registrant's decision-making, particularly if there is to be any dialog or negotiation with the hackers about a ransom payment. It is not hard to see the dilemma facing a registrant between making comprehensive disclosures to investors while simultaneously negotiating with hackers. Adding to this challenge, a materiality determination may itself depend on those negotiations, and could potentially hinge on how negotiations turn out. While the Federal Bureau of Investigation generally discourages making ransom payments to hackers, a registrant may nevertheless find it to be in its best interest to reach an agreement with the hackers in a variety of circumstances, as Caesars evidently concluded (while MGM did not).

---

[8] Caesars Entertainment, Inc., Current Report on Form 8-K, dated September 14, 2023.

[9] News articles have reported that the company paid $15 million of a $30 million demand. *See*, e.g., Sayre, Katherine. "MGM Resorts Refused to Pay Ransom in Cyberattack on Casinos." *The Wall Street Journal*, October 5, 2023.

[10] MGM Resorts International, Current Report on Form 8-K, dated October 5, 2023.

While more time for incident disclosure can facilitate negotiation with hackers and increase the quantity and quality of information available to be disclosed to investors, the SEC has emphasized the risks of unreasonable delay in disclosure. A prompt disclosure within four business days of a materiality determination can be more "bare-bones" and should not be subject to criticism as untimely as long as the detection itself was made within a reasonable time following the attack. To the extent that the materiality determination will take longer than four business days from discovery, a record should be made and the determination process documented to support the decision not to disclose in that period.

Conclusion

In practice, compliance with the new cybersecurity incident disclosure rules will require careful drafting, timely development of information, and close attention to the tension between the goal of alerting investors to security concerns without inadvertently revealing weaknesses to be exploited by the hackers. The final rules allow companies a reasonable time to assess materiality, but this will likely be a tricky determination even in the most straightforward of circumstances. Any such process will be particularly fraught with risk while an attack is ongoing. Companies will be well served to review their incident response plans, confirm they have appropriately-trained and experienced personnel on staff, and engage outside experts to review disclosure controls and procedures and other aspects of preparedness in light of these new requirements.

* * *

If you have any questions about the issues addressed in this memorandum, or if you would like a copy of any of the materials mentioned in it, please do not hesitate to call or email authors David Owen (Partner) at 212.701.3955 or dowen@cahill.com; or Alexa Moses (Associate) at 212.701.3865 or amoses@cahill.com; or email publications@cahill.com.