GIBSON DUNN

SEC Adopts New Rules on Cybersecurity Disclosure for Public Companies

Client Alert | July 31, 2023

On July 26, 2023, the Securities and Exchange Commission ("SEC" or "Commission"), in a 3-to-2 vote, adopted a final rule requiring the disclosure of material cybersecurity incidents and cybersecurity risk management, strategy, and governance by public companies, including foreign private issuers. The Commission's rule proposal, issued in March 2022,[1] was the subject of much commentary and criticism. In response, the Commission made important changes to the required disclosures regarding cybersecurity risk management, strategy, and governance, but the final rule will significantly change the status quo and will impose a substantial burden and introduce complexity to incident response for all public companies.

In summary, the final rule requires: (i) Form 8-K disclosure of material cybersecurity incidents within four (4) business days of the company's determination that the cybersecurity incident is material; (ii) new annual disclosures in Form 10-K regarding the company's cybersecurity risk management and strategy, including with respect to the company's processes for managing cybersecurity threats and whether risks from cybersecurity threats have materially affected the company; and (iii) new annual disclosures in Form 10-K regarding the company's cybersecurity governance, including with respect to oversight by the board and management. The annual disclosures are also required in foreign private issuers' annual reports on Form 20-F, and material cybersecurity incident disclosure will be covered by Form 6-K.

The adopting release is available here, a Fact Sheet from the SEC is available here, and a two page summary prepared by Gibson Dunn is available here. The final rule will become effective 30 days after publication in the Federal Register.

- Most public companies will be required to comply with the Form 8-K incident disclosure requirements beginning on the later of December 18, 2023 and 90 days after the final rule is published in the Federal Register.
- Smaller reporting companies are eligible for an extension for complying with the Form 8-K incident disclosure requirements and have until the later of June 15, 2024 and 270 days after the date the final rule is published in the Federal Register.
- All public companies will be required to comply with the new annual disclosure requirements beginning with the annual report on Form 10-K or 20-F for the fiscal year ending on or after December 15, 2023.

Set forth below is a summary of the final rule and some considerations for public companies.

I. Disclosure of Material Cybersecurity Incidents

***Timing of Disclosure*.** The final rule adds new Item 1.05 to Form 8-K, which requires companies to determine whether a cybersecurity incident[2] is material "without unreasonable delay after discovery of the incident." If a company determines that a cybersecurity incident is material, it is required to disclose the incident within four (4)

Related People

Matthew L. Dolloff

Stephenie Gosnell Handler

Thomas J. Kim

Brian J. Lane

Julia Lapitskaya

Vivek Mohan

Ronald O. Mueller

Michael Scanlon

Michael A. Titera

Lori Zyskowski

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

business days of such determination.

Consistent with the SEC's rule proposal, the final rule uses the date of the materiality determination as the trigger for when the four (4) business day time period begins to run, rather than the date of discovery of the incident—an important distinction.

The timeline for the materiality determination – which must be made "without unreasonable delay" – reflects a change from the rule proposal, which required the determination to be made "as soon as reasonably practicable" after discovery of an incident.[3] Commenters noted that the proposed standard could pressure companies to draw conclusions about incidents with insufficient information. While the SEC revised the timeline in the final rule, the adopting release notes that there may be instances where a company does not have complete information about the incident but knows enough to determine that the incident was material, such as when incidents impact key systems and information or involve unauthorized access to or exfiltration of large quantities of particularly important data. The adopting release states that, in such instances, the materiality determination should not be delayed.[4] Examples of unreasonable delay provided by the adopting release include deferring committee meetings for the responsible committee past the normal time it takes to convene its members or revising existing incident response policies and procedures to support a delayed materiality determination of an ongoing cybersecurity event.[5]

***Scope of Disclosure and Materiality Determination*.** When disclosing the material cybersecurity incident, companies must disclose the material aspects of the nature, scope, and timing of the incident, and the material impact or "reasonably likely" material impact on the company, including on its financial condition and results of operations. If a company determines a cybersecurity incident is material, but the information that is required to be disclosed has not been determined or is unavailable at the time of the required filing, companies must later update the disclosure through a Form 8-K amendment. In contrast to the SEC's rule proposal, which would have provided for updates to appear in subsequent quarterly reports on Form 10-Q, companies must disclose this information within four (4) business days after the company, without unreasonable delay, determines such information or after such information "becomes available."

In the adopting release, the Commission indicated that companies should consider qualitative factors in assessing the material impact of an incident, and indicated that harm to a company's reputation, customer or vendor relationships, or competitiveness, and the possibility of litigation or regulatory investigations or actions, were all examples of potential material impacts on a company.[6]

The final rule's focus on the material aspects of the incident and material impacts on the company represents a narrowing in the scope of required incident disclosure, in comparison to the rule proposal, although compliance will likely present a significant burden to companies actively working to respond to a cybersecurity incident. The SEC's rule proposal would have required disclosure of the specific details of the incident, such as remediation status, whether the incident was ongoing, and whether data were compromised, regardless of materiality. The final rule provides companies with slightly more flexibility, as the instructions to Item 1.05 note that companies "need not disclose specific or technical information" about incident response, systems, networks, or potential vulnerabilities "in such detail as would impede" response or remediation of the incident. However, commentary in the adopting release suggests that the SEC may nonetheless expect companies to disclose sensitive information where it is a significant factor in the determination that a cybersecurity incident is material.[7]

In the adopting release, the Commission took the view that this change in scope alleviates some of the concerns commenters raised about the difficulty of the four (4) business day reporting deadline. The Commission argued that the materiality analysis for most companies will include consideration of the financial impact, so the company will have already developed information about the impact on the company's financial condition and

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

results of operations when Item 1.05 is triggered by the materiality determination.[8] In rejecting a longer deadline suggested by commenters, the SEC asserted that "in the majority of cases registrants will have had additional time leading up to the materiality determination, such that disclosure becoming due less than a week after discovery should be uncommon."[9]

***Exceptions Permitting Reporting Delays*.** The Commission introduced two narrow exceptions that allow for a delay in reporting a material cybersecurity incident on Form 8-K. The only generally applicable exception permitting a delay in reporting applies only if the U.S. Attorney General notifies the SEC in writing that the disclosure poses a substantial risk to national security or public safety. Outside of extraordinary circumstances or an exemptive order issued by the SEC, the maximum delay permitted under this exception will be 60 days.[10]

The second exception is also extraordinarily limited, and applies only to companies subject to the Federal Communications Commission's ("FCC's") notification rule for breaches of customer proprietary network information ("CPNI"). The FCC's rule requires covered entities to notify the United States Secret Service ("USSS") and Federal Bureau of Investigation ("FBI") no later than seven (7) business days after reasonable determination of a CPNI breach and to refrain from disclosing the breach until seven (7) days have passed following notification to the USSS and FBI.[11] The SEC notes that the FCC has proposed amending the CPNI rule to remove this seven (7) business day waiting period, and suggests that this conflict may be eliminated if the FCC's proposed rule is adopted.[12] The SEC's final rule permits companies subject to the notification requirements to delay making the Item 1.05 disclosure up to seven (7) business days following notification to the USSS and FBI, with written notification to the SEC. This exception is being provided as, according to the SEC, this was the only Federal law or regulation that conflicted with Item 1.05.[13]

Additionally, as noted by Commissioner Uyeda during the meeting adopting the final rule, while not an exception built into Item 1.05, the adopting release gives deference to Rule 0-6 under the Securities Exchange Act of 1934 (the "Exchange Act"). Rule 0-6 provides for the omission of information that has been classified by an appropriate department or agency of the Federal government for the protection of the interest of national defense or foreign policy. The adopting release provides that if any information that a registrant would otherwise disclose under Item 1.05 (or pursuant to Item 106 of Regulation S-K, as discussed below) is classified, companies should comply with Rule 0-6, meaning that such information should not be disclosed.[14]

Broad Definition of "Cybersecurity Incident." The final rule broadly defines a cybersecurity incident 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."[15] The final rule also broadly defines "information system" to mean electronic systems "owned or used by" a company, which covers information resources owned by third parties.[16] The SEC's adopting release reaffirmed the SEC's view that an accidental incident is an "unauthorized incident" within the scope of the rule.[17] The SEC acknowledged that the use of the term "jeopardizes" requires a forward-looking assessment of whether the effect of an incident is or is reasonably likely to be material.

The final rule adds the concept of "a series of related unauthorized occurrences"[18] to the definition of "cybersecurity incident," a situation it had proposed to address through a quarterly Form 10-Q reporting requirement. The change means that companies materially affected by a series of related intrusions will still be required to comply with Item 1.05, even when the material impact attributable to each individual intrusion is immaterial by itself. The SEC provided two examples of such a series that would necessitate disclosure under Item 1.05:[19]

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

- The same malicious actor engages in a number of smaller but continuous cyberattacks related in time and form against the same company and collectively, they are either quantitatively or qualitatively material; and
- A series of related attacks from multiple actors exploit the same vulnerability and collectively impede the company's business materially.

***Safe Harbors*.** Consistent with the rule proposal, an untimely filing under Item 1.05 would not result in a loss of Form S-3 eligibility and the failure to file the Item 1.05 Form 8-K would not be deemed to be a violation of Section 10(b) and Exchange Act Rule 10b-5.

II. Cybersecurity Risk Management, Strategy, and Governance Disclosure

Risk Management and Strategy Disclosure. The final rule introduces new Item 106 of Regulation S-K, which will require a description in the Form 10-K of a company's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats[20] in sufficient detail for a reasonable investor to understand those processes. Item 106 states that in providing such disclosure, a company should address, as applicable, the following non-exclusive list of disclosure items:

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

Companies must also describe 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 company, including its business strategy, results of operations, or financial condition and if so, how.

The list of disclosure items under this caption represents a significant paring back from the rule proposal. In the adopting release, the SEC acknowledged concerns on the rule proposal's prescriptiveness and its potential to affect a company's risk management and strategy decision-making.[21] The Commission believes that the formulation in the final rule will not result in companies providing a level of detail that goes beyond material information or that could increase a company's vulnerability.[22] Notably, the final rule requires disclosure of "processes" rather than "policies and procedures," with the SEC noting that the former avoids disclosing operational details that could be used by malicious actors and removes the question of whether companies without written policies and procedures should disclose that fact.[23] Other changes aimed at reducing the prescriptiveness of the rule include the removal of the list of risk types (e.g., intellectual property theft, fraud, etc.) and the removal of certain disclosure items, such as the company's activities undertaken to prevent, detect, and minimize effects of cybersecurity incidents, and the company's business continuity, contingency, and recovery plans in the event of a cybersecurity incident.

Governance Disclosure. Item 106 also requires companies to describe the board of directors' oversight of risks from cybersecurity threats. If applicable, companies must identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the processes by which the board or such committee is informed about such risks. Importantly, the final rule omits the proposed requirement to disclose cybersecurity expertise within the board of directors, although the SEC noted that a company that has determined that board-level expertise is a necessary component to its cyber-risk management would likely provide that disclosure under Item 106.[24]

In addition, companies must describe management's role in assessing and managing the

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

registrant's material risks from cybersecurity threats, with such disclosure addressing, as applicable, the following non-exclusive list of disclosure items:

- 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;
- 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 of directors.

With respect to management's expertise, the instructions to Item 106 provide that it may include "[p]rior work experience in cybersecurity; any relevant degrees or certifications; any knowledge, skills, or other background in cybersecurity."

The final governance disclosure requirements also are significantly less prescriptive than under the rule proposal. Exclusions from the final rule include the proposed requirement to disclose whether and how the board integrates cybersecurity into its business strategy, risk management, and financial oversight, and details such as whether the company has a chief information security officer, the frequency of the board's discussions on cybersecurity, and the frequency with which responsible management positions or committees report to the board on cybersecurity risk. However, the SEC indicated that details such as frequency of discussions or updates may be included in Item 106 disclosure to the extent relevant to an understanding of the board's oversight of risks from cybersecurity threats.[25] While the requirement to disclose whether the company has a chief information security officer was also omitted from the final rule, the SEC noted that the remaining requirement to discuss which management positions or committees are responsible for assessing and managing cybersecurity risk "would typically encompass identification of whether a registrant has a chief information security officer, or someone in a comparable position."[26]

Foreign Private Issuers. The final rule amends Form 20-F to include requirements parallel to Item 106 regarding a foreign private issuer's risk management, strategy, and governance. In addition, the final rule adds "material cybersecurity incidents" to the items that may trigger a current report on Form 6-K. Under the new rule, foreign private issuers will be required to furnish on Form 6-K information about material cybersecurity incidents that the issuers disclose or otherwise publicize in a foreign jurisdiction, to any stock exchange or to security holders.

XBRL Requirements. All new disclosure requirements must be tagged in Inline XBRL (block text tagging for narrative disclosures and detail tagging for quantitative amounts) beginning one year after the initial compliance date for the applicable disclosure requirement.

III. Considerations and Next Steps

Companies should review their cybersecurity incident response playbooks to reflect the processes contemplated under the new Form 8-K requirements. Companies should review and test their procedures for responding to cybersecurity incidents and amend or supplement those procedures as appropriate to address the procedures and attendant documentation contemplated under the new Form 8-K reporting requirements. The final rule provides that the materiality determination for a given cybersecurity incident may not be "unreasonably delayed," so companies should confirm that their disclosure controls and procedures provide for effective communication between the cybersecurity team, the legal team supporting cybersecurity, the legal team responsible for securities disclosure, and the disclosure committee, as well as for appropriate interaction with the board of directors or a responsible committee of the

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

board. Maintaining clearly understood channels of communication will be important in fulfilling the need for a reasonable and timely assessment and escalation of detected cybersecurity incidents, and will assist companies in meeting the cybersecurity incident disclosure requirements. In addition, companies should confirm that their disclosure controls and procedures reflect the considerations discussed in the final rule's adopting release for assessing materiality, including inputs to consider potential reputational harm and damage to customer and vendor relationships. Companies should plan to carefully document both their materiality analysis and the reasonableness of the time that it takes to assess materiality. As Commissioner Peirce noted during the meeting at which the SEC approved the final rule, the days and weeks following detection of a cybersecurity incident are incredibly demanding and stressful on companies, and the new SEC disclosure rules significantly heighten those pressures, but a well-documented playbook that is both sufficiently detailed and sufficiently flexible will serve companies well. In addition, while the final rule did not impose new insider trading procedures relating to cybersecurity incidents, companies should continue to carefully assess that topic during the course of their response to a cybersecurity incident and consider whether and when to suspend any purchases or sales of company securities by the company and by insiders.[27]

Only a narrow set of circumstances qualify for delaying the reporting of material cybersecurity instances and the delay may be difficult to obtain. As described above, the SEC retained the proposed requirement to disclose material cybersecurity incidents within four (4) business days of the company's materiality determination with only narrow exceptions. The only generally applicable exception will require the Attorney General's determination that disclosure poses substantial risk to national security or public safety. While the SEC stated that it has established an interagency communication process, we expect that there may be difficulty in a company obtaining a determination by the Department of Justice, through the Attorney General, that is provided to the Commission in writing within the four (4) business day window following the company's materiality determination, at which point disclosure would be required. It is possible that companies will seek, and the Department of Justice will issue, such a notification of such determination to the Commission in only the most exceptional circumstances. For companies that regularly interact with agencies of the U.S. government responsible for national security, it is possible that certain incidents may be classified and consequently omitted from disclosure.

Companies may need to revisit their processes for managing cybersecurity risk. While the final rule is less prescriptive than the rule proposal, there are still a number of details regarding a company's cybersecurity risk management processes that will need to be disclosed. Companies hoping to avoid disclosure of processes that lack features addressed in the final rule or that appear less robust than those of their peers may want to revisit their processes as they develop their disclosure. Specifically, companies should be aware of the need to describe their engagement of third parties in connection with the risk management process, any processes to oversee and identify risks associated with the use of third-party service providers, and the delegation of responsibility for cybersecurity risks between the board and management. While the SEC did not adopt the requirement to disclose cybersecurity expertise among board members, Commissioner Crenshaw stated that the Commission should continue to consider requiring such disclosure.[28]

Disclosures regarding material cybersecurity incidents and company's risk management processes will require careful drafting. While some of the information required to be disclosed under the final rule has historically been disclosed to regulatory agencies and affected customers, the need to publicly disclose the information in an SEC filing will subject this information to much greater scrutiny and potential liability as a result of possible regulatory enforcement or litigation. These disclosures will require careful drafting to balance the obligation to timely disclose material information without material omission with the important business objective of avoiding unintentionally exposing weaknesses in a company's cybersecurity profile that can be further exploited by malicious actors. While, as discussed above, incident disclosures do not require specific technical information, as Commissioner Peirce noted in her dissent,[29] disclosures could

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

nonetheless provide attackers with important information, such as what the company knows about the incident and the potential financial impact, among other details, and may make it easier for attackers to identify targets. While the final rule allows companies a reasonable time to assess materiality, companies will be well served by avoiding a rushed drafting experience when preparing Form 8-K disclosures by involving inside and outside experts at an early stage. A careful review of companies' cybersecurity incident response playbook, as addressed above, will also facilitate drafting the annual risk management and strategy disclosures. Companies' disclosure controls and procedures should also address post-incident monitoring that allows them to address the highly fraught requirement to annually disclose how risks from previous cyber threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the company. Assuming the final rule's publication in the Federal Register is not substantially delayed, companies will have less than six months to review their existing incident response plans, consider them in light of the new disclosure rules, and make updates as needed.

Companies should coordinate their disclosure of cybersecurity risk management, strategy, and governance with existing disclosures. One of the SEC's stated objectives in adopting the final rule is to consolidate disclosure into a single location in company filings. As noted by the SEC, many companies address cybersecurity risks and incidents in the risk factor sections of their filings, and risk oversight and governance is often addressed in companies' proxy statements. However, the new rule requires disclosure to appear in a newly designated item in Part I of the annual report on Form 10-K and does not allow the disclosures to be incorporated from the proxy statement. Therefore, companies should review their risk factor and proxy statement disclosures when drafting the new discussions of cybersecurity risk management, strategy, and governance for the Form 10-K in order to maintain consistency with the company's past public statements regarding its cybersecurity governance and processes and to assess how those disclosures may be enhanced or revised going forward. We expect companies will continue to include disclosure of cybersecurity governance in their proxy statements, and therefore should consider whether any details disclosed in response to Item 106 should be incorporated into the proxy statement disclosure.

---

[1] For our discussion of the rule proposal, *see* Gibson Dunn Client Alert, SEC Proposes Rules on Cybersecurity Disclosure (Mar. 11, 2022).

[2] The SEC adopted the definition of "cybersecurity incident" used in Regulation S-K for purposes of Item 1.05. Accordingly, "cybersecurity incident" is defined to mean an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a company's information systems that jeopardizes the confidentiality, integrity, or availability of a company's information systems or any information residing therein. "Information systems" is defined to mean electronic information resources, owned or used by the company, 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 company's information to maintain or support the company's operations. Importantly, an unauthorized occurrence on or conducted through an information system that is used by, but not owned by, a company would still be considered a cybersecurity incident, meaning that companies may need to disclose cybersecurity incidents impacting information systems developed by a third party that the company uses.

[3] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 FR 16590, 16624 (Mar. 23, 2022).

[4] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11216 (July 26, 2023) ("Adopting Release") at 37-38.

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

[5] *Id*. at 38.

[6] *Id*. at 29-30.

[7] *See Id*. at 30.

[8] *Id*. at 31-32.

[9] *Id*. at 33.

[10] In extraordinary circumstances, disclosure may be delayed for a final additional period of up to 60 days if the Attorney General notifies the SEC in writing that disclosure continues to pose a substantial risk to national security. Public safety concerns alone would not be a sufficient basis to grant this additional 60-day delay. Id. at 34.

[11] *See* 46 CFR 64.2011(b)(1).

[12] Adopting Release, *supra* note 4, at 42 n.143.

[13] *Id*. at 41-42. This is despite the direct conflict that would arise should an "investigative agency," such as the United States Secret Service, a component agency of the Department of Homeland Security, require a covered telecommunications carrier to delay disclosure consistent with 46 CFR 64.2011(b)(3). The SEC dismisses this conflict by suggesting that the Department of Homeland security may "work with the Department of Justice to seek a delay of disclosure," presumably pursuant to a determination by the Attorney General. *Id*. at 42 n.145.

[14] *Id*. at 35 n.131.

[15] *Id*. at 169-170.

[16] *Id*. at 170.

[17] The Adopting Release mentions "chance technology outages" as an example of an accidental incident, which suggests that a crashed website (which, by definition, jeopardizes the availability of the company's information systems) could meet the definition of a "cybersecurity incident." *Id*. at 72.

[18] *Id*. at 169.

[19] *Id*. at 53.

[20] "Cybersecurity threat" is defined to mean 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.

[21] Adopting Release, *supra* note 4, at 60.

[22] *Id*. at 61.

[23] *Id*.

[24] *Id*. at 85.

[25] *Id*. at 70.

[26] *Id*. at 69-70.

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

[27] The Adopting Release specifically pointed out that the 2018 interpretative guidance issued by the Commission addressing the application of insider trading prohibitions in the context of cybersecurity remains in place. *Id.* at 96.

[28] *See* Commissioner Caroline A. Crenshaw, "Statement on Cybersecurity Adopting Release" (Jul. 26, 2023), available here.

[29] *See* Commissioner Hester M. Peirce, "Harming Investors and Helping Hackers: Statement on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure" (Jul. 26, 2023), available here.

The following Gibson Dunn attorneys assisted in preparing this update: Matthew Dolloff, Nicholas Whetstone, Stephenie Gosnell Handler, Thomas Kim, Brian Lane, Julia Lapitskaya, Vivek Mohan, Ronald Mueller, Michael Scanlon, Alexander Southwell, Michael Titera, and Lori Zyskowski.

Gibson Dunn lawyers are available to assist in addressing any questions you may have about these developments. To learn more, please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any of the following leaders and members of the firm's Privacy, Cybersecurity and Data Innovation, Securities Regulation and Corporate Governance, or Securities Enforcement practice groups:

Privacy, Cybersecurity and Data Innovation Group: Ryan T. Bergsieker – Denver (+1 303-298-5774, rbergsieker@gibsondunn.com) S. Ashlie Beringer – Co-Chair, Palo Alto (+1 650-849-5327, aberinger@gibsondunn.com) Stephenie Gosnell Handler – Washington, D.C. (+1 202-955-8510, shandler@gibsondunn.com) Jane C. Horvath – Co-Chair, Washington, D.C. (+1 202-955-8505, jhorvath@gibsondunn.com) Vivek Mohan – Palo Alto (+1 650-849-5345, vmohan@gibsondunn.com) Ashley Rogers – Dallas (+1 214-698-3316, arogers@gibsondunn.com) Alexander H. Southwell – Co-Chair, New York (+1 212-351-3981, asouthwell@gibsondunn.com) Eric D. Vandevelde – Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)

Securities Regulation and Corporate Governance Group: Elizabeth Ising – Co-Chair, Washington, D.C. (+1 202-955-8287, eising@gibsondunn.com) Thomas J. Kim – Washington, D.C. (+1 202-887-3550, tkim@gibsondunn.com) Brian J. Lane – Washington, D.C. (+1 202-887-3646, blane@gibsondunn.com) Julia Lapitskaya – New York (+1 212-351-2354, jlapitskaya@gibsondunn.com) James J. Moloney – Co-Chair, Orange County (+1 949-451-4343, jmoloney@gibsondunn.com) Ronald O. Mueller – Washington, D.C. (+1 202-955-8671, rmueller@gibsondunn.com) Michael J. Scanlon – Washington, D.C. (+1 202-887-3668, mscanlon@gibsondunn.com) Michael Titera – Orange County (+1 949-451-4365, mtitera@gibsondunn.com) Lori Zyskowski – Co-Chair, New York (+1 212-351-2309, lzyskowski@gibsondunn.com)

Securities Enforcement Group: Richard W. Grime – Co-Chair, Washington, D.C. (+1 202-955-8219, rgrime@gibsondunn.com) Mark K. Schonfeld – Co-Chair, New York (+1 212-351-2433, mschonfeld@gibsondunn.com) David Woodcock – Co-Chair, Dallas (+1 214-698-3211, dwoodcock@gibsondunn.com)

© 2023 Gibson, Dunn & Crutcher LLP Attorney Advertising: The enclosed materials have been prepared for general informational purposes only and are not intended as legal advice. Please note, prior results do not guarantee a similar outcome.

Related Capabilities

Securities Regulation and Corporate Governance

Privacy, Cybersecurity, and Data Innovation

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

GIBSON DUNN

Securities Enforcement

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**