Hogan Lovells

SEC Update

August 10, 2023

This is a commercial communication from Hogan Lovells. See note below.

SEC adopts significant new cybersecurity disclosure requirements

On July 26, the SEC adopted amendments to Regulation S-K and Exchange Act forms requiring public companies to disclose on a current basis material cybersecurity incidents and to disclose annually information regarding their cybersecurity risk management, strategy, and governance.

The amendments will require companies to report a cybersecurity incident on Form 8-K within four business days after the company determines the incident is material. Companies will be required to amend the Form 8-K to provide updated incident disclosure if any information called for in the initial Form 8-K is not determined or available at the time of the initial filing.

The new requirements extend beyond incident reporting to include information intended to enable investors to evaluate companies' ability to manage and mitigate their cybersecurity risk and exposure. Companies will be required to describe in their Form 10-K reports their processes for assessing, identifying, and managing material risks from cybersecurity threats, including whether and how any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations, or financial condition. Companies also will be required to describe the board's role in overseeing cybersecurity risk and management's role in assessing and managing the company's material risks from cybersecurity threats.

The amendments will be effective on September 5, 2023. The amended rules apply to all companies filing reports with the SEC, including foreign private issuers as well as domestic registrants (with the exception of asset-backed issuers). Companies other than smaller reporting companies will first be required to provide the new Form 8-K disclosures beginning on December 18, 2023. Smaller reporting companies will have an additional 180 days to begin complying with the Form 8-K requirements. The Form 10-K disclosures will be due beginning with annual reports filed for fiscal years ending after December 15, 2023.

The SEC's adopting release (Release No. 33-11216) can be viewed here and the fact sheet here.

Background

The adoption of the new requirements follows efforts by the SEC and its staff over the past decade to encourage enhanced disclosure of cybersecurity risks, incidents, and governance through interpretive guidance under the previous disclosure requirements.

Recent regulatory focus

The Division of Corporation Finance published interpretive guidance in 2011 describing the application of specified items of Regulation S-K to cybersecurity risks and incidents and highlighting how the impacts of cybersecurity incidents can affect financial statement presentation.

In an interpretive release published in 2018, the SEC discussed how materiality assessments can shape the timing and content of cybersecurity disclosure. The SEC also addressed board oversight of cybersecurity risk, the importance of adequate disclosure controls and procedures, and the management of insider trading activity and Regulation FD compliance in this context. We discussed the 2011 staff guidance and the 2018 interpretive release in the *SEC Updates* we issued in October 2011 and March 2018.

In recent years, the SEC staff has reinforced this guidance by issuing numerous comment letters regarding cybersecurity disclosure as part of its filing review program. In addition, the SEC has brought enforcement actions against companies for disclosure control failures and misleading disclosures relating to cybersecurity incidents.

Notwithstanding its increased focus on cybersecurity disclosure, the SEC believes that companies may be underreporting cybersecurity incidents and that the value of the published cybersecurity disclosure has been undermined by inconsistencies in timing, coverage, level of detail, and disclosure location. The SEC aims to address these purported deficiencies by adding to its rules prescriptive requirements intended to provide a standardized framework for cybersecurity disclosure.

The SEC confirms in its adopting release that companies should continue to consult the prior interpretive guidance for disclosure determinations and presentations that are not governed by the new requirements. Such topics include cybersecurity-related information in risk factor disclosure under Regulation S-K Item 105, management's discussion and analysis under Item 303, business disclosure under Item 101, and disclosure of relevant legal proceedings under Item 103.

New regulatory action

In its proposing release, which we discussed in our *SEC Update* dated March 25, 2022, the SEC explained that several trends underpin the need for stricter disclosure requirements, including the dependence of an ever-increasing share of economic activity upon electronic systems, a substantial rise in the prevalence of cybersecurity incidents, and the increasing severity of the adverse effects such incidents have on company operations and financial results.

In response to comments on the rule proposal, the SEC made a number of important changes in the final rules, which are discussed in more detail below.

- The rule amendments pertaining to Form 8-K incident disclosure narrow the scope of the required disclosures to focus the disclosure primarily on the impacts of a material cybersecurity incident, rather than on details of the incident itself; eliminate the proposed requirement to report a series of previously undisclosed individually immaterial incidents that become material in the aggregate; require limited updated incident disclosure on an amended Form 8-K rather than on Form 10-Q or 10-K; and allow delayed disclosure of a cybersecurity incident if the United States Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety and notifies the SEC of its determination in writing.
- The final annual disclosure requirements eliminate the proposed requirement to disclose board cybersecurity expertise, and pare back some of the required disclosures addressing risk management, strategy, and governance.

Rule amendments

The new requirements are intended to improve cybersecurity incident reporting and to standardize cybersecurity risk management, strategy, and governance disclosure in public company annual reports.

Cybersecurity incident reporting on Form 8-K

The rule amendments add material cybersecurity incidents to Form 8-K as a mandatory disclosure event under a new Item 1.05 captioned "Material Cybersecurity Incidents."

If a company experiences a cybersecurity incident that it determines to be material, the company must describe, to the extent known at the time of filing, the material aspects of the nature, scope, and timing of the incident, and the incident's material impact or reasonably likely material impact on the company, including its financial condition and results of operations. The SEC underscores that the rule's reference to an incident's impact on a company's financial condition and results of operations is not exclusive, and that the company should consider qualitative factors as well as quantitative factors in assessing the material impact of an incident.

Scope of incident disclosure. The SEC has significantly reduced the scope of new Item 1.05 from its proposal by focusing the disclosure primarily on the impacts of a material cybersecurity incident, rather than on the details of the incident itself. The final requirement represents the SEC's attempt to balance the needs of investors against concerns that disclosure of incident details could empower threat actors and increase a company's vulnerability to cyberattack.

In a further change to the proposal, the amended rule does not require companies to disclose the status of remediation of a cybersecurity incident, whether the incident is ongoing, and whether the company's data were compromised by the incident.

The amended rule requires companies to report only information about a cybersecurity incident that is material. The SEC cautions that some incidents may still necessitate discussion of such impacts as data theft, asset loss, intellectual property loss,

reputational damage, or business value loss, and that the company should consider such impacts as part of its overall materiality analysis.

Item 1.05 includes an instruction clarifying that a company 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 company's response or remediation. The instruction codifies an assurance the SEC made in its proposing release.

Timing of incident disclosure. A company is required to file its Form 8-K within four business days after it determines that a cybersecurity incident is material. An instruction to Item 1.05 provides that a company must make a materiality determination "without unreasonable delay after discovery of the incident," while the proposed rule would have required a company to make a materiality determination "as soon as reasonably practicable after discovery of the incident." The SEC adopted the revised formulation in response to comments contending that the proposed standard might require a company to report a cybersecurity incident before it obtained sufficient relevant information about the incident.

The SEC provides examples of actions that might constitute an unreasonable delay, such as:

- the intentional deferral of a board committee's meeting on the materiality determination past the normal time it takes to convene the committee members; or
- the revision of existing incident response policies and procedures to support a delayed materiality determination.

The SEC states that "adhering to normal internal practices and disclosure controls and procedures will suffice to demonstrate good faith compliance."

The SEC acknowledges that "[i]n the majority of cases, the registrant will likely be unable to determine materiality the same day the incident is discovered." The SEC does not clarify the meaning of "discovery" in this context. As used in various U.S. federal and state breach notification statutes, the term may not necessarily mean the date on which an incident is first identified or detected.

The SEC believes that the reduced scope of required disclosure should alleviate the concerns of many commenters that a filing deadline of four business days after discovery could be too short for adequate reporting. In addition, to the extent any required information is not determined or is unavailable at the time of the required filing, an instruction to Item 1.05 directs the company to include a statement to this effect in the Form 8-K and then to file an amendment to the Form 8-K containing such information within four business days after the company, without unreasonable delay, determines such information, or within four business days after such information becomes available.

In the proposing release, the SEC requested comment on whether to allow companies to delay reporting of a material cybersecurity incident where the Attorney General determines that a delay is in the interest of national security. The final rule includes a delay provision, although on a much more limited basis than suggested by some commenters.

Under the rule, if the Attorney General determines that the disclosure of an incident poses a substantial risk to national security or public safety and notifies the SEC of its determination in writing, a company may delay disclosure of the incident for a period specified by the Attorney General, up to 30 days following the date on which the company was otherwise required to provide the disclosure. The delay may be extended for an additional period of up to 30 days if the Attorney General determines that disclosure continues to pose a substantial risk to national security or public safety and notifies the SEC of its determination in writing. In extraordinary circumstances, disclosure may be further delayed for a final additional period of up to 60 days, beyond which the SEC may grant further relief through an exemptive order.

The final rule also includes a limited exception permitting delayed reporting by a company subject to a rule promulgated by the Federal Communications Commission if the company is required by that rule to delay disclosing a data breach.

Companies are not otherwise permitted to delay disclosure beyond the Form 8-K deadline because of the existence of an ongoing internal or external investigation of the incident or because of a conflict with other federal or state law. The filing deadline may create tension with managing notifications of the incident to other regulators, particularly under state breach notification laws that require notification "without unreasonable delay" or "as expeditiously as practicable," standards that historically have been understood to mean up to 30 days or longer after the incident discovery date. The SEC notes that its rule does not preclude any federal or state agency from

requesting that the Attorney General determine that the disclosure poses a substantial risk to national security or public safety and communicate that determination to the SEC.

Definition of cybersecurity incident. A "cybersecurity incident" potentially triggering Form 8-K reporting is defined in a new Item 106 of Regulation S-K 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 SEC emphasizes that this definition should be "construed broadly."

The SEC added the phrase "or a series of related unauthorized occurrences" to the definition of "cybersecurity incident" to reflect that "cyberattacks sometimes compound over time, rather than present as a discrete event." If a company determines that it has been materially affected by what may appear as a series of related cyber intrusions, Item 1.05 will be triggered even if the material impact or reasonably likely material impact could be parceled among the multiple intrusions to render each intrusion by itself immaterial. The SEC provides the following two non-exclusive examples of such a situation:

- the same malicious actor engages in a number of smaller but continuous cyberattacks related in time and form against the same company which collectively 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 to a material extent.

The SEC clarifies that an accidental occurrence may be a cybersecurity incident under the definition, even if there is no confirmed malicious activity. For example, if a company's customer data are accidentally exposed, allowing unauthorized access to such data, the data breach would constitute a cybersecurity incident that would necessitate a materiality analysis to determine whether Item 1.05 disclosure is required.

The SEC's definition of cybersecurity incident is not the same as the definitions used by other regulatory bodies. As a result, occurrences that companies may not historically have classified as "incidents" may now be considered cybersecurity incidents for SEC disclosure purposes.

Materiality assessments. The SEC confirms that the materiality of a cybersecurity incident would be assessed consistently with existing materiality principles under the securities laws. Accordingly, a cybersecurity incident would be deemed material if there is a substantial likelihood that a reasonable investor would consider information about the incident important in deciding whether to buy, hold or sell the company's securities, or if there is a substantial likelihood that a reasonable investor would view information about the incident as having significantly altered the "total mix" of information made available. Echoing the materiality discussion in its 2018 interpretive release, the SEC emphasizes that this determination should take into account both qualitative and quantitative factors.

In recognition of "the circumstances that will surround Item 1.05 disclosures," the rules provide that failure to report a cybersecurity incident on Form 8-K in a timely manner will not result in loss of the company's eligibility to file a short-form registration statement on Securities Act Form S-3, so long as Form 8-K reporting is current at the time the Form S-3 is filed. The rules also add Item 1.05 to the list of Form 8-K items requiring rapid materiality determinations that are eligible for a limited safe harbor from liability under Exchange Act Section 10(b) and Rule 10b-5 thereunder if they are the subject of untimely filings.

Cybersecurity governance reporting on Form 10-K

The SEC adopted a new Item 106 of Regulation S-K captioned "Cybersecurity" that prescribes governance disclosures, and amended Form 10-K to require companies to report the information required by the new item. In adopting the requirements, the SEC weighed investors' needs to understand a company's governance of cybersecurity risks in sufficient detail to inform an investment or voting decision against concerns that the requirements could impel companies to adopt specific or inflexible cybersecurity-risk governance practices or organizational structures.

Risk management processes. New Item 106(b)(1) requires companies to describe their "processes," if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. The item identifies as a non-exclusive list of items companies should address in their disclosure:

- 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.

The SEC declined to include prevention and detection activities, continuity and recovery plans, and previous incidents as enumerated disclosure topics under Item 106(b)(1), and revised the proposed disclosure of third-party service providers to reduce the level of required detail.

The SEC has substituted the word "processes" for "policies and procedures," as proposed, in identifying the scope of this discussion "to avoid requiring disclosure of the kinds of operational details that could be weaponized by threat actors, and because the term 'processes' more fully [en]compasses registrants' cybersecurity practices than 'policies and procedures,' which suggest formal codification."

New Item 106(b)(2) requires 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 company, including its business strategy, results of operations, or financial condition, and if so, how.

Board oversight of cybersecurity risk. Item 106(c)(1) requires companies to describe the board of directors' oversight of risks from cybersecurity threats. 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.

Management's role in managing cybersecurity risk. Item 106(c)(2) requires companies to describe management's role in assessing and managing material risks from cybersecurity threats. In this description, companies should address, as applicable, disclosure items such as those presented in the following non-exclusive list:

- 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.

Changes from the proposed rule on governance disclosures. In response to comments, the SEC streamlined Item 106(c) to require less detailed disclosure than it had proposed. Item 106(c)(1) on board oversight does not require disclosure regarding the frequency of board discussions or whether and how the board or committee considers cybersecurity risks as part of its business strategy, risk management, and financial oversight. The required disclosure under Item 106(c)(2) regarding management's role is limited to actions addressing material risks from cybersecurity threats. In a change to the proposal, companies are not specifically required to disclose information regarding their designated chief information security officer.

The SEC did not add a materiality qualifier to the requirement to describe board oversight because it believes that if a board of directors determines to oversee a particular risk, the fact of such oversight itself is material to investors. By contrast, the SEC added a materiality qualifier to the disclosure of management's role required by Item 106(c)(2) because management addresses many more matters, and the SEC believes that management action with respect to non-material matters is likely not material to investors.

Other proposed disclosure requirements not adopted

The SEC did not adopt a proposed requirement that would have obligated companies to disclose on Forms 10-Q and 10-K any material changes, additions, or updates to previous cybersecurity incident disclosures made pursuant to Item 1.05 of Form 8-K. The final rule instead provides that companies must report updated incident disclosure only in limited circumstances and in an amendment to the Form 8-K that disclosed the incident.

The SEC reminds companies, however, that, in accordance with its existing rules and with principles underlying the federal securities laws, they may be required to correct prior disclosure that they determine was untrue (or omitted a material fact necessary to make the disclosure not misleading)

at the time it was made, or to update disclosure that becomes materially inaccurate after it is made. A company should consider whether it may need to revisit prior disclosure when investigating a cybersecurity incident and should be aware of the requirement under new Item 106(b)(2) to 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.

The SEC also did not require, as proposed, incident reporting when a series of previously undisclosed individually immaterial cybersecurity incidents becomes material in the aggregate.

Finally, the SEC did not adopt its proposal that would have required companies to identify in their annual proxy statements which of their directors, if any, have cybersecurity expertise and to describe the nature of that expertise.

Structured data requirements for cybersecurity disclosure

To improve the accessibility and availability of cybersecurity disclosure, the final rules require all disclosures under Item 1.05 of Form 8-K, Item 106 of Regulation S-K, and Item 16K of Form 20-F to be provided in Inline XBRL. The structured data requirement includes block text tagging of narrative disclosures and detail tagging of quantitative amounts. The SEC expects that this tagging will facilitate more efficient large-scale analysis and comparison of cybersecurity information across companies and time periods, and better searchability of cybersecurity information.

Companies must comply with the structured data requirements beginning one year after their mandatory initial compliance with the disclosure requirements.

Application of rules to other issuers

Foreign private issuers. The rule amendments extend the requirements for enhanced cybersecurity incident and annual cybersecurity disclosures to foreign private issuers through amendments to Forms 6-K and 20-F.

To elicit timely cybersecurity incident disclosure, the SEC amended Form 6-K to add "material cybersecurity incident" to the events that may trigger a filing. Form 6-K requires disclosure of material information – including with respect to topics specified in the form – which the foreign private issuer makes or is required to make public under home jurisdiction law, files or is required to file under stock exchange rules, or distributes or is required to distribute to its security holders. Form 6-K, as amended, does not require disclosure of all material cybersecurity incidents, but rather those otherwise required to be disclosed by the Form 6-K filing triggers noted above.

The proposal also requires annual cybersecurity disclosures by foreign private issuers generally consistent with those required by domestic companies. The SEC amended Form 20-F to add a new Item 16K requiring foreign private issuers to disclose cybersecurity governance information on an annual basis.

Smaller reporting companies. To help mitigate the cost burdens smaller reporting companies will face in complying with the new requirements, those companies are not required to begin complying with Item 1.05 of Form 8-K until June 15, 2024.

Looking ahead

Consistent with the approach the SEC has taken in other recent rulemakings, the rule amendments emphasize more rapid and detailed reporting and incorporate prescriptive requirements to promote uniform and comparable disclosures. As in other recent rules, both proposed and adopted, the SEC also seeks to expand the scope of required disclosures to encompass a description of relevant governance policies and practices.

Although the SEC underlines the expected benefits of enhanced disclosure to investors, it also recognizes the potential adverse impacts the new reporting requirements could have on companies. The required disclosure could increase rather than decrease the vulnerability of public companies to cybersecurity incidents as a result of the insights the disclosures could give into a company's cybersecurity practices and readiness.

The SEC acknowledges that there is some risk of the disclosure of a cybersecurity incident "tipping off threat actors," and that disclosure "could, potentially, provide a road map for future attacks, and, if the underlying security issues are not completely resolved, could exacerbate the ongoing attack." The SEC also acknowledges that risk management, strategy, and governance disclosure could provide malicious actors information about which companies have weak processes related to cybersecurity risk management and allow such malicious actors to "determine their targets accordingly." The SEC believes that the modifications it made to the proposed requirements

should mitigate such risks and that the final rules appropriately balance such risks against investors' need for improved cybersecurity disclosure.

Companies should consider whether they need to augment their disclosure controls and procedures to ensure they are able, in a timely fashion, to identify cybersecurity incidents as defined by the SEC, evaluate their potential materiality, and prepare the newly required disclosures. As part of this review, companies may find it necessary to revisit their incident response plans and processes, particularly regarding severity classifications and reporting escalation thresholds. Companies also should critically reappraise existing cybersecurity risk management policies and related governance arrangements, which will be exposed to more searching regulatory and investor scrutiny.

Contributors

Alan L. Dye (co-editor)
Partner, Washington, D.C.
Securities & Public Company Advisory
T +1 202 637 5737
alan.dye@hoganlovells.com

Richard Parrino (co-editor)
Partner, Washington, D.C.
Securities & Public Company Advisory
T +1 202 637 5530
richard.parrino@hoganlovells.com

John B. Beckman
Partner, Washington, D.C.
Securities & Public Company Advisory
T +1 202 637 5464
john.beckman@hoganlovells.com

Kevin K. Greenslade
Partner, Northern Virginia
Securities & Public Company Advisory
T +1 703 610 6189
kevin.greenslade@hoganlovells.com

Ann C. Kim
Partner, Los Angeles
Investigations, White Collar and Fraud
T +1 310 785 4711
ann.kim@hoganlovells.com

Paul Otto
Partner, Washington, D.C.
Privacy and Cybersecurity
T +1 202 637 5887
paul.otto@hoganlovells.com

Peter M. Marta
Partner, New York
Privacy and Cybersecurity
T +1 212 918 3528
peter.marta@hoganlovells.com

Allison Holt Ryan
Partner, Washington, D.C.
Litigation
T +1 202 637 5872
allison.holt-ryan@hoganlovells.com

Brendan R. Oldham
Senior Associate, Washington, D.C.
Securities & Public Company Advisory
T +1 202 637 7814
brendan.oldham@hoganlovells.com

Spencer Leroux
Associate, Northern Virginia
Securities & Public Company Advisory
T +1 703 610 6127
spencer.leroux@hoganlovells.com

Additional contacts

Steven J. Abrams
Partner, Philadelphia
T +1 267 675 4671
steve.abrams@hoganlovells.com

Richard Aftanas
Partner, New York
T +1 212 918 3267
richard.aftanas@hoganlovells.com

Tifarah Roberts Allen
Partner, Washington, D.C.
T +1 202 637 5427
tifarah.allen@hoganlovells.com

Jessica A. Bisignano
Partner, Philadelphia
T +1 267 675 4643
jessica.bisignano@hoganlovells.com

David W. Bonser
Partner, Washington, D.C.
T +1 202 637 5868
david.bonser@hoganlovells.com

Glenn C. Campbell
Partner, Baltimore, Washington, D.C.
T +1 410 659 2709 (Baltimore)
T +1 202 637 5622 (Washington, D.C.)
glenn.campbell@hoganlovells.com

David Crandall
Partner, Denver
T +1 303 454 2449
david.crandall@hoganlovells.com

John P. Duke
Partner, Philadelphia, New York
T +1 267 675 4616 (Philadelphia)
T +1 212 918 5616 (New York)
john.duke@hoganlovells.com

Allen Hicks
Partner, Washington, D.C.
T +1 202 637 6420
allen.hicks@hoganlovells.com

Paul Hilton
Senior Counsel, Denver, New York
T +1 303 454 2414 (Denver)
T +1 212 918 3514 (New York)
paul.hilton@hoganlovells.com

Eve N. Howard
Partner, Washington, D.C.
T +1 202 637 5627
eve.howard@hoganlovells.com

William I. Intner
Partner, Baltimore
T +1 410 659 2778
william.intner@hoganlovells.com

Bob Juelke
Partner, Philadelphia
T +1 267 675 4615
bob.juelke@hoganlovells.com

Paul D. Manca
Partner, Washington, D.C.
T +1 202 637 5821
paul.manca@hoganlovells.com

Michael E. McTiernan
Partner, Washington, D.C.
T +1 202 637 5684
michael.mctiernan@hoganlovells.com

Stephen M. Nicolai
Partner, Philadelphia
T +1 267 675 4642
stephen.nicolai@hoganlovells.com

Brian C. O'Fahey
Partner, Washington, D.C.
T +1 202 637 6541
brian.ofahey@hoganlovells.com

Tiffany Posil
Partner, Washington, D.C.
T +1 202 637 3663
tiffany.posil@hoganlovells.com

Leslie (Les) B. Reese, III
Partner, Washington, D.C.
T +1 202 637 5542
leslie.reese@hoganlovells.com

Richard Schaberg
Partner, Washington, D.C., New York
T +1 202 637 5671 (Washington, D.C.)
T +1 212 918 3000 (New York)
richard.schaberg@hoganlovells.com

Michael J. Silver
Partner, New York, Baltimore
T +1 212 918 8235 (New York)
T +1 410 659 2741 (Baltimore)
michael.silver@hoganlovells.com

Andrew S. Zahn
Partner, Washington, D.C.
T +1 202 637 3658
andrew.zahn@hoganlovells.com

Elizabeth (Liz) L. Banks
Counsel, Washington, D.C.
T +1 202 637 2523
elizabeth.banks@hoganlovells.com

J. Nicholas Hoover
Counsel, Baltimore
T +1 410 659 2790
nick.hoover@hoganlovells.com

Alicante
Amsterdam
Baltimore
Beijing
Berlin**
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dublin
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta *
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Munich
New York
Northern Virginia
Paris
Philadelphia
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.

*Our associated offices
**Legal Services Center

www.hoganlovells.com