Morgan Lewis | White Paper

SEC PROPOSES CYBERSECURITY RISK MANAGEMENT RULES FOR ADVISERS AND FUNDS

February 2022

www.morganlewis.com

SEC PROPOSES CYBERSECURITY RISK MANAGEMENT RULES FOR ADVISERS AND FUNDS

The US Securities and Exchange Commission (SEC) recently proposed a comprehensive framework of cybersecurity-related rules and amendments for investment advisers and investment companies. Although advisers and funds may have already implemented many of the requirements, some, such as incident reporting, are likely to prove burdensome and make the landscape surrounding cybersecurity risk management and compliance even more complex.

With respect to investment companies, the scope of the requirements is somewhat unclear—as are what findings a board must make to approve a fund's cybersecurity program and on whom the board may rely in doing so.

SUMMARY AND BACKGROUND

On February 9, the SEC proposed new and amended rules and forms under the Investment Advisers Act of 1940 (Advisers Act) and the Investment Company Act of 1940 (1940 Act) that would require investment advisers and funds to adopt and implement written cybersecurity policies and procedures, report significant cybersecurity incidents, disclose significant cybersecurity risks, and create and maintain related records (Proposal).[1]

The SEC believes that advisers and funds face a growing number of cybersecurity risks and threats due to their reliance on interconnected systems and networks, both directly and through various service providers, as well as from their use of digital engagement tools and other client-facing technologies. Cybersecurity incidents can cause substantial financial, operational, legal, and reputational harm to advisers and funds, and clients and investors can also be harmed by cybersecurity incidents. The SEC and its staff have previously addressed cybersecurity preparedness, and we have discussed such releases.[2]

The SEC noted in the Proposal that Regulation S-P already requires that advisers adopt written, reasonably designed policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. In addition, the SEC noted that in complying with the Advisers Act's fiduciary and regulatory obligations, advisers often contemplate their particular cybersecurity risks and develop policies and procedures designed to address those risks. Finally, the Federal Trade Commission's Safeguards Rule[3] was recently amended to provide more specific security requirements applicable to non-SEC-regulated financial institutions and may also apply to private funds.

Despite the prior guidance and current requirements, the SEC stated that, because there are no existing SEC rules that specifically require advisers or funds to adopt and implement comprehensive cybersecurity risk management programs, there is a concern that some advisers and funds have not implemented such

[1] *See* Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, Rel. Nos. 33-11028, 34-94197, IA-5956, IC-34497 (Feb. 9, 2022). As used in the Proposal and in this White Paper, "funds" means registered investment companies and business development companies.

[2] *See* Morgan Lewis LawFlash, SEC Observations from Recent Cybersecurity Examinations Identify Best Practices (Aug. 15, 2017); Morgan Lewis White Paper, Proactive Approach to Cybersecurity (Oct. 2015).

[3] *See* Morgan Lewis LawFlash, Expanded Safeguards Rule Applicable to More Financial Institutions; Gives More Specificity on Security Requirements (Nov. 19, 2021).

programs, and that some programs that have been implemented lack critically important elements. The SEC noted in the proposing release that in a recent survey of financial firms, 58% of the respondents self-reported "underspending" on cybersecurity (the SEC also cited a report that, somewhat surprisingly, non-bank financial firms are some of the biggest spenders on cybersecurity measures).

The SEC also expressed concern that clients of investment advisers and investors in funds may not be receiving sufficient cybersecurity information, particularly with respect to cybersecurity incidents, to help ensure that they are making informed investment decisions. Moreover, the SEC believes that, in the face of ever-increasing cybersecurity risk, advisers and funds should report certain cybersecurity incidents to the SEC to assist in its oversight role.

To address these concerns, the SEC proposes to require that advisers and funds adopt and implement cybersecurity risk management policies and procedures, report significant cybersecurity incidents to the SEC, disclose information about cybersecurity risks and significant incidents, and prepare and maintain related records.

PROPOSAL DETAILS

Cybersecurity Risk Management Policies and Procedures

Proposed new Rule 206(4)-9 under the Advisers Act and proposed new Rule 38a-2 under the 1940 Act (together, the Proposed Rules) are key elements of the Proposal. The Proposed Rules would require all investment advisers that are registered with the SEC, or required to be registered with the SEC, and all funds that are registered with the SEC to adopt and implement written policies and procedures that are reasonably designed to address cybersecurity risks.

The SEC acknowledged that advisers and funds would need flexibility to ensure that their policies and procedures are consistent with the nature and scope of their business, operations, and specific cybersecurity risks, and the Proposed Rules, although they enumerate in considerable detail the elements those policies and procedures must include, were meant by the SEC to provide that flexibility. Under the Proposed Rules, advisers and funds would be tasked with determining the person or group of people responsible for implementing and administering their cybersecurity policies and procedures, which could be a third party, as long as such third party is subject to appropriate oversight.

Required Elements

The Proposed Rules list certain elements that must be incorporated into all adviser and fund cybersecurity policies and procedures, including the following:

1. **Risk Assessment**. Advisers and funds would be required to periodically assess, categorize, prioritize, and draft written documentation of the cybersecurity risks associated with adviser and fund information systems, respectively, and the adviser or fund information residing in those systems. The Proposed Rules would also require advisers and funds to reassess and reprioritize their cybersecurity risks periodically, although there is no proposed requirement for such reassessments to be performed at specific intervals.
2. **User Security and Access**. The Proposed Rules would require all cybersecurity policies and procedures to include controls designed to minimize user-related risks and prevent unauthorized access to information and systems, including by (i) requiring standards of behavior for individuals authorized to access adviser or fund information systems and any adviser or fund information residing therein, such as an acceptable use policy; (ii) identifying and authenticating individual

users, including implementing authentication measures that require users to present a combination of two or more credentials for access verification; (iii) establishing procedures for the timely distribution, replacement, and revocation of passwords or methods of authentication; (iv) restricting access to specific adviser or fund information systems or components thereof and adviser or fund information residing therein solely to individuals requiring access to such systems and information as is necessary for them to perform their responsibilities and functions on behalf of the adviser or fund; and (v) securing remote access technologies used to interface with adviser or fund information systems.

3. **Information Protection**. Advisers and funds would also be required to monitor information systems and protect information from unauthorized access or use, based on a periodic assessment of their information systems and the information that resides on those systems. The proposing release also emphasizes that advisers and funds would be required to oversee any service providers that receive, maintain, or process adviser or fund information, or are otherwise permitted to access their information systems and any information residing on those systems. Additionally, under the Proposed Rules advisers and funds would have to document that they require their service providers, pursuant to a written contract, to implement and maintain appropriate cybersecurity measures similar to those that the advisers and funds must address in their own cybersecurity policies and procedures.

4. **Cybersecurity Threat and Vulnerability Management**. Pursuant to the Proposed Rules, advisers and funds would be required to detect, mitigate, and remediate "cybersecurity threats"[4] and "cybersecurity vulnerabilities"[5] with respect to their information and systems. The SEC recommends that advisers and funds seek to detect cybersecurity threats and vulnerabilities through ongoing monitoring, and that mitigating and remediating such threats and vulnerabilities could include, for example, patching hardware and software vulnerabilities in a timely manner and maintaining a process to track and address reports of vulnerabilities.

5. **Cybersecurity Incident Response and Recovery**. Advisers and funds would also be required to have measures to detect, respond to, and recover from a "cybersecurity incident."[6] As part of this requirement, advisers and funds would be expected to have policies and procedures reasonably designed to ensure (i) continued operations of the fund or adviser; (ii) the protection of adviser information systems and the fund or adviser information residing therein; (iii) external and internal cybersecurity incident information sharing and communications; and (iv) reporting of significant cybersecurity incidents to the SEC. In the event of a cybersecurity incident, advisers and funds would also have to prepare written documentation of the incident, including their response and recovery from the incident.

[4] "Cybersecurity threat" means any potential occurrence that may result in an unauthorized effort to adversely affect the confidentiality, integrity, or availability of an adviser's (or a fund's) information systems or any adviser (or fund) information residing therein. *See* Proposed Rules 206(4)-9 and 38a-2.

[5] "Cybersecurity vulnerability" means a vulnerability in an adviser's (or a fund's) information systems, information system security procedures, or internal controls, including vulnerabilities in their design, configuration, maintenance, or implementation that, if exploited, could result in a cybersecurity incident. *See* Proposed Rules 206(4)-9 and 38a-2.

[6] "Cybersecurity incident" means an unauthorized occurrence on or conducted through an adviser's (or a fund's) information systems that jeopardizes the confidentiality, integrity, or availability of an adviser's (or a fund's) information systems or any adviser (or fund) information residing therein. *See* Proposed Rules 206(4)-9 and 38a-2.

The Proposed Rules' required elements are substantially similar to the Federal Trade Commission's (FTC's) Safeguards Rule, which in turn closely tracks recently enacted regulations by state financial regulators, such as the New York Department of Financial Services Cybersecurity Regulations and the Massachusetts Cybersecurity Regulations. Additionally, the Proposed Rules' required elements share many characteristics with the US Department of Labor's recently issued guidance outlining "cybersecurity program best practices" for ERISA plan service providers.[7] Uniformity among cybersecurity requirements is helpful for businesses, but many advisers and funds may have already implemented some or all of the Proposed Rules' requirements, and therefore the utility of the new requirements, aside from serving as an enforcement tool, is somewhat questionable.

In fact, Commissioner Peirce expressed a similar concern in a statement following her dissent on the Proposal.[8] She noted that detailed cybersecurity requirements (or a cybersecurity breach) could lead to an enforcement action against an adviser or fund, even if the adviser or fund made a reasonable attempt to comply with the requirements. Commissioner Peirce also stated her opposition to grounding Proposed Rule 206(4)-9 in the Advisers Act's anti-fraud provision because, among other reasons, the fraudulent acts the SEC's Proposal seeks to prevent are not ones in which the adviser is the perpetrator, but the victim. She also pointed out that the language of the proposed rule would, taken literally, prohibit an adviser from providing investment advice to its clients during any period in which the adviser's cybersecurity policies and procedures were deficient.

Annual Reviews and Written Reports

On at least an annual basis, all advisers and funds would be required to (1) review and assess the design and effectiveness of their cybersecurity policies and procedures, including whether such policies and procedures reflect changes in cybersecurity risk over the time period covered by the review; and (2) prepare a written report. The written report must, at a minimum, describe the annual review, assessment, and any control tests performed; explain the results thereof; document any cybersecurity incident that occurred since the date of the last report; and discuss any material changes to the policies and procedures since the date of the last report.

Board Oversight

Proposed Rule 38a-2 would require a fund's board of directors, including a majority of its independent directors, to oversee the implementation and administration of the fund's cybersecurity policies and procedures. Specifically, a fund's board would be required to initially approve the fund's policies and procedures and review the annual written report regarding cybersecurity incidents and material changes to the fund's policies and procedures. The SEC emphasized in the proposing release that board oversight of a fund's cybersecurity risk management should not be a passive activity. For example, the SEC recommends that each fund's board consider what level of oversight is necessary for the fund's service providers, based on the fund's operations and current practices.

In the proposing release, the SEC states that the requirement of fund board approval is intended to facilitate the board's oversight of the fund's cybersecurity program and to provide "accountability." The SEC asks in its request for comment whether board approval should be required, and that seems at least open to question. Most fund board members are not cybersecurity experts. It is unclear the extent to which a board, in approving cybersecurity policies and procedures, may rely on assessments by in-house

[7] *See* Morgan Lewis LawFlash, A Deeper Dive into the DOL's First-of-Its-Kind Cybersecurity Guidance (Apr. 23, 2021).

[8] *See* Commissioner Hester M. Peirce, Statement on Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies (Feb. 9, 2022).

experts employed by the fund's adviser. Will boards feel the need to retain their own experts? The SEC states that directors may satisfy their obligation with respect to the initial approval by reviewing summaries prepared by the people who administer the fund's cybersecurity policies and procedures. This may merely permit a board's use of summaries rather than the detailed policies and procedures themselves, and probably does not authorize broader reliance on those who administer the fund's cybersecurity program.

Because the procedures are required to be "reasonably designed to address cybersecurity risks," one might have inferred that was the standard for the board's approval. Apparently, however, that may not be the case. In its request for comment, the SEC asks whether board approval should be based on some particular finding, such as that the procedures are reasonably designed to prevent violations of federal securities laws or to address the fund's cybersecurity risks—suggesting that the proposed rule does not (at least not yet) mandate a particular standard. Directors will undoubtedly be seeking further guidance from the SEC as to what standard they need to apply in approving a cybersecurity program, and how they can get comfortable that the standard is met.

The Proposed Rules focus on protecting "adviser information" and "adviser information systems" and "fund information" and "fund information systems." Most funds of course, other than the relatively few internally managed funds, do not have any systems of their own, but instead rely on service providers, including investment advisers, administrators, transfer agents, and custodians, to carry out their functions and to hold their information.

The definition of "fund information systems" refers to the information resources "owned or used by the fund." It is not clear whether that comprehends the systems of service providers—they are not owned by the fund, but are they used "by" the fund, or merely on behalf of the fund? If service provider systems are not "fund information systems," then a fund may not have such systems and the scope of its own procedures might be limited accordingly. If they are, that would potentially significantly expand the scope of a fund's procedures. In its requests for comment, the SEC asks whether fund boards should be required to approve the cybersecurity policies and procedures of certain of the fund's service providers.

Reporting of Significant Cybersecurity Incidents to the SEC

The SEC also proposed new Rule 204-6 under the Advisers Act, which would require advisers to report significant cybersecurity events that affect the adviser, or its fund or private fund clients, to the SEC on a confidential basis. Advisers would have to submit proposed Form ADV-C to the SEC promptly, but in no event more than 48 hours, after having a reasonable basis to conclude that a "significant adviser cybersecurity incident"[9] or a "significant fund cybersecurity incident"[10] had occurred or is occurring.

[9] A "significant adviser cybersecurity incident" means a cybersecurity incident, or a group of related cybersecurity incidents, that significantly disrupts or degrades the adviser's ability, or the ability of a private fund client of the adviser, to maintain critical operations, or leads to the unauthorized access or use of adviser information, where the unauthorized access or use of such information results in (1) substantial harm to the adviser or (2) substantial harm to a client, or an investor in a private fund, whose information was accessed. This could potentially apply even if a limited number of clients or investors, or possibly even a single client or investor, was substantially harmed. *See* Proposed Rule 204-6.

[10] A "significant fund cybersecurity incident" means a cybersecurity incident, or a group of related cybersecurity incidents, that significantly disrupts or degrades the fund's ability to maintain critical operations or leads to the unauthorized access or use of fund information, where the unauthorized access or use of such information results in substantial harm to the fund or to an investor whose information was accessed. As with respect to an adviser incident, this could potentially apply even if a limited number of investors, or possibly even a single investor, was substantially harmed. *See* Proposed Rule 38a-2.

Note that a filing might be required even if the adviser had some uncertainty as to whether an incident had in fact occurred, or as to its significance—in order to be required to file Form ADV-C, the adviser need only have a "reasonable basis." Although the timing requirement for reporting is very aggressive when compared to the reporting requirements of other regulators, the SEC stated that it believes that advisers should have sufficient information to respond to the proposed questions by the time the filing is due.

This requirement is very similar to the incident notification requirement recently adopted by the three federal banking agencies,[11] except that, under Proposed Rule 204-6, the time period in which a report must be made is shorter. The FTC also released proposed notification requirements for financial institutions under its remit.[12] The plethora of existing notification requirements, all to different regulators, with different timing and triggers, add to the complex compliance burden faced by financial institutions (especially those overseen by multiple regulators) under very difficult circumstances.

Form ADV-C is structured as a series of check-the-box and fill-in-the-blank questions, and it is intended to capture identifying information about the adviser and background information about the incident, including whether the adviser notified law enforcement or another government agency of the cybersecurity incident. Following the initial submission, advisers would also be required to amend any previously filed Form ADV-C, within 48 hours, after information previously reported becomes materially inaccurate, if additional or new material information about a previously reported incident is discovered, and after resolving a previously reported incident or closing an internal investigation relating to a previously reported incident.

The SEC explained in the proposing release that it believes that the reporting of significant cybersecurity incidents will assist its efforts to monitor and assess the impact of such incidents on advisers and funds, and also help it evaluate and respond to the potential systemic risks affecting the financial markets. The proposing release also states that the SEC or its staff could issue analyses and reports that are based on aggregated, non-identifying Form ADV-C data.

Disclosure of Cybersecurity Risks and Incidents

In addition to SEC reporting, the Proposal also includes amendments to existing forms that are designed to enhance the public disclosure of advisers and funds regarding their cybersecurity risks and incidents. In particular, the proposed amendments are to Form ADV Part 2A for advisers, and to Forms N-1A, N-2, N-3, N-4, N-6, N-8B-2, and S-6 for funds. We had discussed the previous SEC guidance on cybersecurity disclosures.[13]

If the Proposal is adopted, a new Item 20 titled "Cybersecurity Risks and Incidents" would be added to Form ADV Part 2A. This new item would require advisers to describe, in plain English, the cybersecurity risks that could materially affect the advisory services they offer and how they assess, prioritize, and address cybersecurity risks based on their business. An adviser would also have to disclose any cybersecurity incidents that occurred within the last two fiscal years that significantly disrupted or degraded the adviser's ability to maintain critical operations, or that led to the unauthorized access or use of adviser information, and that resulted in substantial harm to the adviser or its clients. Additionally, the

[11] *See All Things FinReg*, Federal Banking Agencies Adopt New Computer-Security Incident Notification Requirements (Dec. 22, 2021).

[12] *See* Morgan Lewis LawFlash, Expanded Safeguards Rule Applicable to More Financial Institutions; Gives More Specificity on Security Requirements (Nov. 19, 2021).

[13] *See* Morgan Lewis LawFlash, SEC Issues Guidance on Cybersecurity Disclosures (Feb. 28, 2018).

Proposal contains an amendment to Rule 204-3(b) under the Advisers Act that would require an adviser to deliver interim brochure amendments to existing clients promptly if the adviser adds disclosure of a cybersecurity incident to its brochure, or materially revises information already disclosed in its brochure about such an incident.

The amendments under the Proposal would also require funds to disclose any significant fund cybersecurity incidents that have occurred in the last two fiscal years. Specifically, a fund would have to describe each such incident including, to the extent known, (1) the entity or entities affected; (2) when the incident was discovered and whether it is ongoing; (3) whether any data was stolen, altered, or accessed or used for any other unauthorized purpose; (4) the effect of the incident on the fund's operations; and (5) whether the fund or service provider has remediated or is currently remediating the incident.

The new information would have to be tagged using the Inline eXtensible Business Reporting Language (Inline XBRL), which would result in an additional compliance burden for unit investment trusts since they are currently not subject to any requirements to report using Inline XBRL. In the proposing release, the SEC suggested that to the extent funds are not already doing so, they should consider cybersecurity risks when preparing risk disclosures for their registration statements. The SEC also recommends that funds include a discussion of cybersecurity risks and significant fund cybersecurity incidents in their reports to shareholders, if such risks and incidents materially affected the performance of the fund during the period covered by the report.

Recordkeeping

As part of the Proposal, advisers and funds would be required to maintain (for five years, with the first two years in an easily accessible place) the following records, as applicable:

1. A copy of their cybersecurity policies and procedures that are in effect, or were in effect at any time within the past five years
2. A copy of the written report documenting the annual review of their cybersecurity policies and procedures in the last five years
3. A copy of any Form ADV-C filed in the last five years
4. Records documenting the occurrence of any cybersecurity incident, including any records related to any response and recovery from such an incident, in the last five years
5. Records documenting any cybersecurity risk assessment in the last five years

NEXT STEPS

Advisers and funds should compare their current cybersecurity policies and procedures to the requirements of the Proposal and identify areas for comment. The SEC has provided a short comment period ending 30 days from publication in the *Federal Register* or April 11, 2022, whichever is later. Those who wish to comment should do so soon.

Morgan Lewis has a global team of lawyers who regularly assist advisers and funds with their regulatory compliance needs, including those related to securities, privacy, and cybersecurity regulations. Please contact us if you would like assistance with the review of your firm's policies or preparation of a comment letter.

Morgan Lewis

CONTACTS

If you have any questions or would like more information on the issues discussed in this White Paper, please contact any of the following Morgan Lewis lawyers:

Boston

Lea Anne Copenhefer	+1.617.951.8515	leaanne.copenhefer@morganlewis.com
Lance C. Dial	+1.617.341.7727	lance.dial@morganlewis.com
Barry N. Hurwitz	+1.617.951.8267	barry.hurwitz@morganlewis.com
Roger P. Joseph	+1.617.951.8247	roger.joseph@morganlewis.com
Jeremy B. Kantrowitz	+1.617.951.8458	jeremy.kantrowitz@morganlewis.com
Paul B. Raymond	+1.617.951.8567	paul.raymond@morganlewis.com
Toby R. Serkin	+1.617.951.8760	toby.serkin@morganlewis.com
Mari Wilson	+1.617.951.8381	mari.wilson@morganlewis.com

Chicago

Lauren Z Groebe	+1.312.324.1478	lauren.groebe@morganlewis.com

Houston

Catherine North Hounfodji	+1.713.890.5120	catherine.hounfodji@morganlewis.com

London

Pulina Whitaker	+44.20.3201.5550	pulina.whitaker@morganlewis.com

Los Angeles

Taylor C. Day	+1.213.612.7367	taylor.day@morganlewis.com

New York

Jedd H. Wider	+1.212.309.6605	jedd.wider@morganlewis.com
Elizabeth L. Belanger	+1.212.309.6353	elizabeth.belanger@morganlewis.com
Abigail Bertumen	+1.212.309.6019	abigail.bertumen@morganlewis.com
Martin Hirschprung	+1.212.309.6837	martin.hirschprung@morganlewis.com

Orange County

Laurie A. Dee	+1.714.830.0679	laurie.dee@morganlewis.com
Jonathan J. Nowakowski	+1.714.830.0640	jonathan.nowakowski@morganlewis.com

Philadelphia

Ezra D. Church	+1.215.963.5710	ezra.church@morganlewis.com
David W. Freese	+1.215.963.5862	david.freese@morganlewis.com
Sean Graber	+1.215.963.5598	sean.graber@morganlewis.com
Kristin M. Hadgis	+1.215.963.5563	kristin.hadgis@morganlewis.com
Timothy W. Levin	+1.215.963.5037	timothy.levin@morganlewis.com
Christine M. Lombardo	+1.215.963.5012	christine.lombardo@morganlewis.com
John J. O'Brien	+1.215.963.4969	john.obrien@morganlewis.com
Gregory T. Parks	+1.215.963.5170	gregory.parks@morganlewis.com
Terese M. Schireson	+1.215.963.4830	terese.schireson@morganlewis.com

Pittsburgh

Elizabeth S. Goldberg	+1.412.560.7428	elizabeth.goldberg@morganlewis.com

Matthew H. Hawes	+1.412.560.7740	matthew.hawes@morganlewis.com
Michael Gorman	+1.412.560.7476	michael.gorman@morganlewis.com
San Francisco		
Reece Hirsch	+1.415.442.1422	reece.hirsch@morganlewis.com
Susan D. Resley	+1.415.442.1351	susan.resley@morganlewis.com
Silicon Valley		
Mark L. Krotoski	+1.650.843.7212	mark.krotoski@morganlewis.com
Washington, DC		
Ronald W. Del Sesto, Jr.	+1.202.739.6023	ronald.delsesto@morganlewis.com
Laura E. Flores	+1.202.373.6101	laura.flores@morganlewis.com
Ivan P. Harris	+1.202.739.5692	ivan.harris@morganlewis.com
Thomas S. Harman	+1.202.373.6725	thomas.harman@morganlewis.com
W. John McGuire	+1.202.373.6799	john.mcguire@morganlewis.com
Christopher D. Menconi	+1.202.373.6173	christopher.menconi@morganlewis.com
Courtney C. Nowell	+1.202.739.5223	courtney.nowell@morganlewis.com
Steven W. Stone	+1.202.739.5453	steve.stone@morganlewis.com
Beau Yanoshik	+1.202.373.6133	beau.yanoshik@morganlewis.com
Mana Behbin	+1.202.373.6599	mana.behbin@morganlewis.com
Magda El Guindi-Rosenbaum	+1.202.373.6091	magda.elguindi-rosenbaum@morganlewis.com
Monica L. Parry	+1.202.373.6179	monica.parry@morganlewis.com
Dr. Axel Spies	+1.202.739.6145	axel.spies@morganlewis.com
Drew Cleary Jordan	+1.202.739.5962	drew.jordan@morganlewis.com

ABOUT US

Morgan Lewis is recognized for exceptional client service, legal innovation, and commitment to its communities. Our global depth reaches across North America, Asia, Europe, and the Middle East with the collaboration of more than 2,200 lawyers and specialists who provide elite legal services across industry sectors for multinational corporations to startups around the world. For more information about us, please visit www.morganlewis.com.