

# Key Considerations for the 2024 Annual Reporting Season

November 18, 2024

As November comes to an end, the busy annual reporting and proxy season begins for many public companies. In this Client Update, we highlight key considerations for public companies when preparing their annual reports on Form 10-K or Form 20-F, including a new exhibit filing requirement for insider trading policies. For a checklist covering these considerations, see the Annex to this update.

---

## Key Takeaways

- For the first time, companies will be required to file their insider trading policy as an exhibit to their Form 10-K or Form 20-F and to disclose certain information about their insider trading policies and procedures.
- In 2024, the U.S. Securities and Exchange Commission's (the "SEC") Division of Enforcement continued to focus on cybersecurity and artificial intelligence ("AI") disclosures. Companies should review these disclosures and refresh their risk factors to address emerging risks, actual cybersecurity incidents and to ensure they accurately reflect the company's use of AI.
- Company counsel should keep abreast of potential changes to disclosure requirements related to climate change and board diversity in light of ongoing litigation and the new federal administration.
- Consistent with prior years, the SEC has remained focused on non-GAAP measures. Companies should regularly review their use of non-GAAP measures for compliance with Regulation G, Item 10(e) of Regulation S-K, and related guidance issued by the staff of the SEC's Division of Corporation Finance.
- The SEC remained active in its rulemaking and enforcement activities in 2024. How the SEC's priorities change following the transition to the new administration remains to be seen, but a move away from the SEC's current agenda is foreseeable.

Even so, efforts to change course will likely take time and public companies are well advised to continue being vigilant of their disclosures.

---

## New Insider Trading Policy Disclosure Requirements Applicable to Annual Reports

For public companies with a calendar year end, compliance with new disclosure requirements relating to insider trading policies and procedures begins with the 2024 Form 10-K or Form 20-F or related proxy statement. Item 601 requires public companies to file any insider trading policy as an exhibit to their annual report on Form 10-K or Form 20-F. This requirement can also be satisfied if the company's insider trading policies are contained in its code of ethics and the code of ethics is filed as an exhibit to the Form 10-K or Form 20-F.

In addition, new Item 408(b) of Regulation S-K and new Item 16J of Form 20-F require public companies to disclose whether they have adopted insider trading policies and procedures governing trading in the company's securities by employees, officers or directors, or by the company itself, that are reasonably designed to promote compliance with insider trading laws, rules and regulations and any applicable listing standards. Companies that have not adopted such policies and procedures are required to explain why they have not done so. A company can incorporate by reference in its Form 10-K the information required under Item 408(b) from a definitive proxy statement if the proxy statement is filed within 120 days of the end of the fiscal year.

In our [Insider Trading and Disclosure Update](#) published in July 2024, we recommended that companies consider updates and refinements to their insider trading policies in anticipation of the new disclosure requirements, including to address the use of insider information to trade in securities of "economically-linked" companies, commonly referred to as a "shadow trading." Additionally, the new disclosure requirement will require companies to disclose whether they have trading policies applicable to transactions by the company, which has not historically been a common feature of insider trading policies. We recommend companies take care not to adopt a trading policy that imposes an undue burden on company activity. For example, companies could consider including a statement within an existing trading policy that it is the policy of the issuer to comply with all applicable insider trading laws, rules and regulations. This should allow companies to comply with the policy disclosure requirements, without unintentionally and unduly limiting companies' ability to engage in appropriate transactions in their own securities.

---

## Recap of Cybersecurity Disclosures

In 2023, the SEC adopted final rules on cybersecurity risk management, strategy, governance and incident disclosure for public companies. The rules introduced new annual disclosure requirements relating to cybersecurity risk-management processes and cybersecurity governance, which took effect beginning with Form 10-K or Form 20-F relating to fiscal years ending on or after December 15, 2023 (*i.e.*, for a calendar year end issuer, the 2023 Form 10-K or Form 20-F filed in 2024). Beginning with annual reports for fiscal years ending on or after December 15, 2024, Regulation S-K Item 106 disclosure must be tagged in Inline eXtensible Business Reporting Language.

Among other disclosure requirements under Item 106 of Regulation S-K, public companies are required to describe their process for assessing, identifying and managing material risks from cybersecurity threats as well as the board's oversight of, and management's role and expertise in, assessing and managing material risks posed by cybersecurity threats.

On June 24, 2024, the SEC released five new Compliance and Disclosure Interpretations ("C&DIs") relating to the disclosure of material cybersecurity incidents under Item 1.05 of Form 8-K. While the fact patterns underlying the new C&DIs focus on Form 8-K disclosure and ransomware, companies should consider the guidance generally in analyzing disclosure obligations for cybersecurity events. For more information followed by the full text of the new C&DIs, see our [Debevoise Debrief—SEC Releases New Guidance on Material Cybersecurity Incident Disclosure](#).

The SEC issued three comment letters regarding Form 10-K Item 1C cybersecurity disclosure in 2024, all of which noted the failure to include Item 1C cybersecurity disclosure. In response, all three companies filed an amendment on Form 10-K/A, adding Item 1C disclosure.

During 2024, the SEC's Division of Enforcement also continued its aggressive stance with regards to cybersecurity disclosure. On October 22, 2024, the SEC announced settled charges in separate actions against four technology companies who had been downstream victims of the 2020 SUNBURST cyber-attack. Although the disclosures and statements at issue in these four actions pre-dated the SEC's adoption of the final cybersecurity disclosure rule, companies should consider these cases as reflecting the SEC's views on materiality assessment and disclosure decisions regarding cybersecurity incidents. In light of the charges and the SEC's continued review of cybersecurity disclosure, companies preparing to file their Form 10-K or Form 20-F should review their cybersecurity disclosures and refresh their risk factors to address emerging cybersecurity risks as well as actual incidents.

For further information on the SEC’s announced settlements, see our [Debevoise in Depth—SEC Charges Four Companies for Misleading Cyber Disclosures](#).

### Trends in Cybersecurity Risk Management and Governance

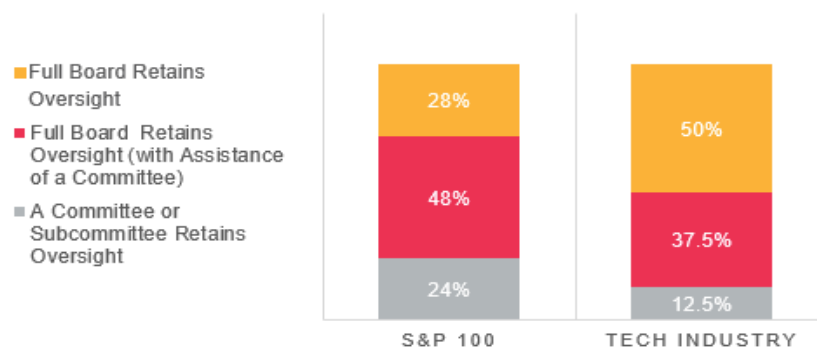
Following the 2023 annual reporting season, we surveyed the annual reports filed by 50 S&P 100 companies and identified the following trends:

#### Structure of Board Oversight

The structure of board oversight of cybersecurity governance generally falls into one of the following three categories:

- the board has primary oversight of cybersecurity governance;
- the board has primary oversight of cybersecurity governance, with assistance from a specified committee; or
- a committee or subcommittee of the board has primary oversight of cybersecurity governance.<sup>1</sup>

The chart below shows the breakdown of how the companies surveyed structured their cybersecurity governance.



Among the sample group, technology companies were more likely than others to retain oversight of cybersecurity at the full board, rather than a committee. To the extent committees or subcommittees had primary oversight over cybersecurity, that responsibility most commonly resided with the audit committee.

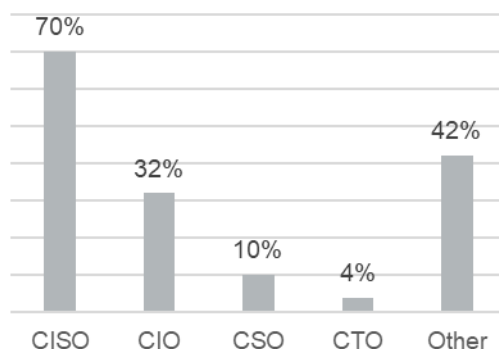
<sup>1</sup> All references to S&P 100 are to a sample of 50 S&P 100 companies as of February 29, 2024.

### Frequency of Cybersecurity Reports to the Board

The survey revealed that over 25% of S&P 100 companies reported that their boards are updated on cybersecurity matters “regularly,” with over 35% of technology companies reporting that their boards are updated “periodically.” A majority used qualitative language to describe the frequency of updates, rather than quantitative specificity. This approach may be desirable to preserve greater flexibility. In our experience, it is common for the board to receive a detailed update on cybersecurity matters one to two times a year, with additional reports on an as-needed basis.

### The Role of Management

As illustrated below, most S&P 100 companies cite more than one managerial role as being responsible for cybersecurity risk management.<sup>2</sup>



In addition, while 84% of S&P 100 companies disclosed management’s credentials, this was often done in generic terms, avoiding disclosure of individual names, and those individual’s degrees or certifications.

### Disclosing Material Cybersecurity Incidents

Overwhelmingly, S&P 100 companies expressly disclosed that they have not experienced material cybersecurity incidents either within Item 1C of Form 10-K (or Item 16K of Form 20-F) or in their risk factor section. Companies are cross-referencing their risk factors to describe cybersecurity threats, though most companies do not specify a specific timeline during which they have not experienced a material cybersecurity incident.

---

<sup>2</sup> Percentages do not add to 100% due to companies citing multiple roles.

---

## Update on Board Diversity Requirements

### Nasdaq Diversity Requirement Challenge in Fifth Circuit

Nasdaq requires companies listed on its exchanges to disclose board diversity information and meet diversity requirements. Companies are required to disclose diversity statistics regarding their board of directors and to have, or explain why they do not have, at least two diverse directors, including one who self-identifies as female and one who self-identifies as either an “underrepresented minority” or “LGBTQ+.”

In October 2023, a three-judge panel of the Fifth Circuit upheld Nasdaq’s board diversity rule, but the rule is once again under review by the Fifth Circuit *en banc* and the timing of the court’s decision remains uncertain. Currently, Nasdaq listed companies are required to have at least one diverse director or provide an explanation as to why they do not have such a director. Companies listed on the Nasdaq Global Select or Global markets must have at least two diverse directors by December 31, 2025 or provide the requisite explanation. Companies listed on the Nasdaq Capital Market must have at least two diverse directors by December 31, 2026 or provide the requisite explanation.

### California Board Diversity Challenged in Federal Court

On September 30, 2020, California passed California Assembly Bill No. 979 (“AB 979”), which required public companies headquartered in the state to include a minimum number of directors from “underrepresented communities” or be subject to fines for violating the statute. On May 15, 2023, the Eastern District of California ruled AB 979 violated 42 U.S.C. §1981, a federal statute governing equal rights under the law, and the Equal Protection Clause of the U.S. Constitution’s Fourteenth Amendment.

The decision could impact pending appeals in California state court from another decision invalidating AB 979 and a separate ruling invalidating Senate Bill 826 (“SB 826”), California’s gender-diversity statute for corporate boards. SB 826, if upheld on appeal, will require publicly held corporations with headquarters in California to have a minimum number of female directors on their boards within specified time periods.

Although the future of AB 979 and SB 826 and their respective compliance deadlines remain uncertain, companies that fall within the scope of the legislation should consider how they plan to comply should the laws be upheld.

---

## Other Disclosure “Hot Topics”

### Artificial Intelligence (“AI”)

Public companies should prepare for continued SEC scrutiny in connection with their AI disclosures, policies and procedures. We expect the SEC to continue to focus on “AI-washing”—the making of unsubstantiated or hyperbolic AI disclosures. Companies adding disclosure about their use of AI to annual reports should ensure that sufficient support exists for all statements. And as AI continues to develop, and companies consider expanding their use of AI, it will be critical to ensure that oversight of those uses, the associated risks and related disclosures, keeps pace.

In 2024, the SEC demonstrated its willingness to use existing federal securities laws to bring AI-related fraud cases. In October 2024, the SEC announced settled charges against Rimar Capital USA, Inc., Rimar Capital, LLC (“Rimar LLC”), founder and CEO Itai Liptz, and director Clifford Boro under the antifraud provisions of the federal securities laws for allegedly making materially false and misleading statements to investors, including but not limited to statements about Rimar LLC’s purported use of AI to perform automated trading for advisory clients. Andrew Dean, Co-Chief of the SEC Enforcement Division’s Asset Management Unit, issued a statement warning that “[a]s AI becomes more popular in the investing space,” the SEC “will continue to be vigilant and pursue those who lie about their firms’ technological capabilities and engage in ‘AI washing.’” The settlement follows the SEC’s earlier AI-related fraud cases in 2024 against two investment advisers, Delphia (USA) Inc. and Global Predictions INC., and against the founder and CEO of tech startup Joonko Diversity, Inc.

In light of the SEC’s focus on AI, public companies should review their disclosures and other public statements regarding the use of AI to ensure accuracy.

### Non-GAAP Financial Measures

Non-GAAP financial measures remain a significant focus of the SEC, exemplified by the continued issuance of comment letters in 2024, following the revised Compliance and Disclosure Interpretations published in December 2022.

As in previous years, recent comment letters have focused on the presentation of the most directly comparable GAAP financial measure with “equal or greater prominence” as the non-GAAP financial measure.

Companies should regularly review their use of non-GAAP measures for compliance with Regulation G, Item 10(e) of Regulation S-K and related guidance issued by the staff of the SEC’s Division of Corporation Finance.

## Climate-Related Disclosures

On April 4, 2024, the SEC stayed implementation of its climate-related disclosure rules—the Enhancement and Standardization of Climate-Related Disclosures for Investors—pending judicial review in the Eighth Circuit. The future and ultimate scope of the rule and timeline for implementation remain uncertain, particularly in light of the new federal administration.

Nevertheless, it remains important for companies to review their existing climate-related disclosures and ensure appropriate support exists for any climate-related claims as well as consistency with any sustainability reports or other climate-related statements they publish. In its comment letters to companies relating to climate-related disclosures, the SEC has consistently rejected conclusory statements regarding materiality, instead requiring registrants to provide the SEC with detailed analysis regarding how materiality determinations were made.

In 2024, the SEC continued its efforts to clamp down on “greenwashing.” For example, on September 10, 2024, the SEC announced settled charges against a beverages and consumer products company for making inaccurate statements regarding the recyclability of its single-use beverage products.

Additionally, California’s climate-related disclosure rules, Senate Bill 253, the Climate Corporate Data Accountability Act, and Senate Bill 261, the Climate-Related Financial Risk Act, continue to face legal challenge in the U.S. District Court for the Central District of California. Though the future of the rules remains uncertain, their implementation is not stayed pending the outcome of the litigation. We recently published a Debevoise Debrief—California Climate Disclosure Bills Signed into Law, available [here](#).

## Geopolitical Conflict Disclosures

In May 2022, the SEC published a [sample comment letter](#) reminding public companies that they may have disclosure obligations related to the direct or indirect impact of Russia’s invasion of Ukraine. The comment letter states that public companies should provide detailed disclosure regarding any direct or indirect exposure to Russia or Ukraine through the company’s supply chains, operations, investments, assets or business relationships.

The Division of Corporation Finance has not published a sample comment letter on the conflict in the Middle East as of the date of this update; however, it is likely that the SEC’s view regarding disclosure is the same. As such, companies that have direct or indirect exposure to the conflict in the Middle East; operations, investments or assets in



the conflict area; or business relationships with companies that do should evaluate any material impacts or risks of future impacts related to the conflict in the Middle East.

---

## Practical Tips for Annual Reporting Season

### Trends in the Role of Disclosure Committees

Disclosure committees are essential for safeguarding accuracy and compliance in the disclosure process. Although they are not legally required to do so, disclosure committees tend to be a greater asset to a company when they support disclosure controls and procedures as opposed to solely supporting financial reporting controls. While their structure varies across companies, the influence of disclosure committees is being recognized as pivotal in cultivating a corporate ethos of transparency and ethical conduct as they expand their oversight.

A recent survey of 135 public companies conducted by the Society for Corporate Governance and Ernst & Young LLP found that 96% of companies surveyed confirmed they have a formal disclosure committee or some comparable group with similar responsibilities.

Additionally, the survey found that most disclosure committees operate under a formal charter. Thirty-four percent of companies reported that these charters are approved by the disclosure committee itself, while a handful of other companies have charters approved by their chief financial officers or audit committees. Twenty-one percent of companies surveyed indicated that their charters are approved by multiple internal committees or groups.

Most disclosure committees surveyed meet on a quarterly basis while also meeting on an as-needed basis for significant events and filings. Disclosure committees report increasing their review of non-GAAP financial measures and human capital disclosures—likely a reaction to increasing SEC scrutiny and the anticipated human capital disclosure rules. A minority of companies surveyed reported that their disclosure committees also now review disclosure about AI and similar emerging technologies.

Though disclosure committees are increasingly reviewing cybersecurity disclosures, the survey revealed that most committees defer to management or legal teams to determine the materiality of cybersecurity incidents.

Overall, disclosure committees continue to be an important cornerstone of corporate governance as their roles expand to include competencies beyond the traditional profile of preparing disclosures and verifying financial statements, such as review of

cybersecurity, human capital management, enterprise risk management, and ethics and compliance disclosures. Companies should consider how the structure and responsibilities of their disclosure committees can be curated to effectively handle emerging issues.

### **“Pure Omissions” Are Not Actionable under Rule 10b-5(b)**

In April 2024, the Supreme Court handed down its decision in *Macquarie Infrastructure Corp. v. Moab Partner, L.P.*, confirming that a failure to make disclosure that is responsive to a disclosure requirement, standing alone, does not give rise to a private right of action under Rule 10b-5(b). The decision arose in the context of Item 303 of Regulation S-K (“Management’s discussion and analysis of financial condition and results of operations,” or “MD&A”) but has reach beyond Item 303, standing for the broader principle that Rule 10b-5(b) does not support pure omissions theories based on alleged violation of a disclosure requirement.

Although the Court declined to expand the scope of the private right of action under Rule 10b-5(b), public companies are also subject to SEC review and enforcement action regarding omissions in MD&A and so must remain vigilant about their disclosures. Moreover, the Court’s decision does not foreclose plaintiffs from filing claims concerning Item 303 of Regulation S-K under a “half-truths” theory—*i.e.*, that the information omitted from MD&A renders other statements made misleading. In addition, pure omissions theories remain viable under Section 11 of the Securities Act of 1933, as amended (the “Securities Act”).

### **Updated Process for Expiring Confidential Treatment Orders**

On January 8, 2024, the SEC Division of Corporation Finance updated the guidance on confidential treatment applications and confidential treatment order extensions made pursuant to Rule 406 of the Securities Act and Rule 24b-2 of the Securities Exchange Act of 1934, as amended. In particular, the guidance set out the options available to companies that have confidential treatment orders that are about to expire.

There are three alternatives, depending on whether the confidential treatment order was initially granted more or less than three years ago: companies may refile an unredacted exhibit; request an extension; or transition to the streamlined process that was created by the SEC in 2019.

For more information on the updated guidance, see our [Debevoise Debrief—SEC Updates Processes for Expiring Confidential Treatment Orders](#).

## Improvements to EDGAR System Orders

On September 27, 2024, the SEC adopted a proposal that aims to enhance the security of the Electronic Data Gathering, Analysis and Retrieval (“EDGAR”) system and improve filers’ access and account-management capabilities. Most significantly, EDGAR filers will no longer be able to use one account for the entire company. Instead, each individual logging into the EDGAR system for the filer must have their own account and credentials. Under the new system, each filer must authorize and maintain at least two individuals with individual account credentials as administrators to manage the filer’s account and make submissions on EDGAR.

For more information on the SEC’s improvement to EDGAR, see our [Debevoise Digest: Securities Law Synopsis—October 2024](#).

## Delaware Law Updates

Based on recent developments in Delaware corporate law, public companies should consider in connection with the upcoming annual reporting season:

- Review the language of advance notice bylaws, rights agreements and equity incentive plans in light of *Kellner v. AIM ImmunoTech Inc.* and other recent decisions. In *Kellner*, the Delaware Court of Chancery reviewed several advance notice bylaw provisions and held that several of these provisions were invalid. The court noted that onerous bylaws that stray far afield from the promotion of order and disclosure risk invalidation. Companies should review the language of the aforementioned documents to identify language similar to what was at issue in *Kellner*.
- Remember that boards may ratify agreements under new Section 147 of the Delaware General Corporation Law (the “DGCL”). Senate Bill 313 enacted a new Section 147 of the DGCL, which provides that whenever the DGCL requires board approval of any “agreement, instrument or document,” such document may be approved in “final form or in substantially final form.” In addition, the board can ratify its prior approval of any agreement referenced in any certificate filed with the Delaware Secretary of State at any time before such filing becomes effective. Accordingly, if there is any uncertainty about whether an agreement was in final form when approved by the board, the board can comply with the DGCL by ratifying the finalized agreement before its effectiveness.

Our monthly Debevoise Digests, where we summarize recent disclosure issues, are available on our [Insights & Publications Page](#).

**Annex: Issuer Checklist & Filing Deadlines—At a Glance**

Topic	Summary of Change	Relevant Form 10-K Section	Issuer Checklist	Further Resources
Insider Trading	Issuers must disclose whether they have adopted insider trading policies and procedures and, if so, file their insider trading policy as an exhibit to their Form 10-K or Form 20-F.	Part IV, Item 15	<p><b>Insider Trading Policy and Procedure:</b></p> <ul style="list-style-type: none"> <li>Describe insider trading policies and procedures</li> <li>Describe how the policies and procedures apply to employees, officers, directors or the issuer itself</li> </ul> <p><b>Include Insider Trading Policy as an Exhibit:</b></p> <ul style="list-style-type: none"> <li>File policies and procedures as exhibits</li> </ul>	<a href="#">Insider Trading &amp; Disclosure Update—Special Issue</a>
Cybersecurity Risk Management and Governance	In July 2023, the SEC adopted final rules that require periodic disclosures about cybersecurity risk management and governance.	Part I, Item 1C	<p><b>Cybersecurity Risk-Management Processes:</b></p> <ul style="list-style-type: none"> <li>Describe risk-management programs.</li> <li>Describe whether any risks for cybersecurity threats, current or previous, have materially affected or are likely to materially affect business strategy, operations or financial conditions.</li> </ul> <p><b>Cybersecurity Governance:</b></p> <ul style="list-style-type: none"> <li>Describe the board’s oversight of cybersecurity threats.</li> <li>Describe management’s role in assessing and managing risks posed by cybersecurity threats.</li> <li>To the extent members of management are involved, describe their prior work experience, education or knowledge, skills or other background in cybersecurity.</li> </ul>	<a href="#">SEC Releases New Guidance on Material Cybersecurity Incident Disclosure</a>
Other Disclosure Considerations	Issuers should keep in mind these disclosure considerations when preparing their Form 10-K or Form 20-F.	As Applicable	<ul style="list-style-type: none"> <li>AI Adoption, Risk Management and Governance</li> <li>Non-GAAP Financial Measures</li> <li>Climate-Related Disclosures</li> <li>Geopolitical Conflict Disclosures</li> </ul>	<p>AI: <a href="#">SEC Announces Settled Charges Against Rimar Capital Entities and Owner for Defrauding Investors in “AI-washing” Scheme Governance Round-Up Issue 13</a>;</p> <p>Non-GAAP: <a href="#">SEC Maintains Its Focus on Non-GAAP Financial Measures</a></p> <p>Climate-Related Disclosures: <a href="#">SEC Issues Long-Awaited Climate-Related Disclosure Rule</a></p> <p>Geopolitical Conflict: <a href="#">SEC Sample Comment Letter</a></p>

---

## Form 10-K Filing Deadlines

- Large Accelerated Filer: March 3, 2025 (or 60 days after fiscal year end)
- Accelerated Filer: March 17, 2025 (or 75 days after fiscal year end)
- Non-Accelerated Filer: March 31, 2025 (or 90 days after fiscal year end)

\* \* \*

Please do not hesitate to contact us with any questions.



**Eric T. Juergens**  
Partner, New York  
+ 1 212 909 6301  
etjuergens@debevoise.com



**Benjamin R. Pedersen**  
Partner, New York  
+ 212 909 6121  
brpedersen@debevoise.com



**Paul M. Rodel**  
Partner, New York  
+ 212 909 6478  
pmrodel@debevoise.com



**Alice Gu**  
Associate, New York  
+ 1 212 909 6057  
agu@debevoise.com



**Victoria S. Li**  
Associate, New York  
+ 1 212 909 6644  
vsli@debevoise.com



**Amy Pereira**  
Associate, New York  
+ 1 212 909 6413  
apereira@debevoise.com



**Justin A. Norris**  
Law Clerk, New York  
+ 212 909 6424  
janorris@debevoise.com

*This publication is for general information purposes only. It is not intended to provide, nor is it to be used as, a substitute for legal advice. In some jurisdictions it may be considered attorney advertising.*