Client Alert | US Public Company Advisory Group

Key Considerations for Updating 2023 Annual Report Risk Factors

December 21, 2023

With the 2023 annual report season upon us, it is time for companies to take stock of risk factors for 10-Ks and 20-Fs, and consider whether recent economic, political, technological, and regulatory developments have had (or are expected to have) a material impact on their business, financial condition and operating results.[1]

As a starting point, this alert features (i) a list of key developments that U.S. public companies should consider as they update risk factors in Part I and (ii) critical drafting considerations in Part II. Each company will, of course, need to assess its own material risks and tailor its risk factor disclosure to its particular circumstances.

Part I: Key Developments to Consider when Updating 2023 Annual Report Risk Factor Disclosures

1. Cybersecurity

Cybersecurity incidents, data misuse, and ransomware attacks continue to proliferate and become more sophisticated, and in July 2023, the SEC adopted mandatory cybersecurity disclosure rules that require a new section of annual reports (in Part I, Item IC of Form 10-Ks and Item 16K of Form 20-Fs) to disclose information regarding their cybersecurity risk management, strategy, and governance.[2] As Director of the Division of Corporation Finance Erik Gerding noted, "cybersecurity risks have increased alongside the ever-increasing share of economic activity that depends on electronic systems, the growth of remote work, the ability of criminals to monetize cybersecurity incidents, the use of digital payments, and the increasing reliance on third party service providers for information technology services, including cloud computing technology." Further, the cost to companies and their investors of cybersecurity incidents is rising at an increasing rate.

Although the SEC's new cybersecurity rules do not directly impact risk factor disclosure, cyber disclosure will need to be consistent across the annual report and accurately reflect a company's cybersecurity risk profile. Companies should therefore reassess their cybersecurity risk factor disclosure as they prepare the newly required cybersecurity disclosure, particularly with respect to overlapping aspects of the requirements. For example, under the newly adopted cybersecurity disclosure required in annual reports, companies must describe their cybersecurity risk management processes and 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 them, including their business strategy, results of operations, or financial condition.

Previously, the SEC had issued guidance in February 2018 that specifically addressed cybersecurity risk factors and called on companies to "disclose previous or ongoing cybersecurity incidents or other past events in order to place discussions of these risks in the appropriate context," and specified a number of other issues to consider for risk factor disclosure, including "costs associated with maintaining cybersecurity protections" and "third party

---

1 See Item 105 of Regulation S-K, available here.

2 For more information, see our prior alert, "SEC Adopts Mandatory Cybersecurity Disclosure Rules." For a summary, see Statement on Cybersecurity Disclosure, Erik Gerding (December 14, 2023).

supplier and service provider risks." The 2018 guidance as it pertains to risk factors remains a useful point of consideration.[3]

In reassessing cybersecurity risk factor disclosures, companies should also take note of recent enforcement actions and comment letters from the SEC. For example, the SolarWinds SEC enforcement action focused in large part on risk factor disclosure failures, noting that the company's SEC filings "contained general, high-level risk disclosures" that "failed to address known risks." SolarWinds' SEC filings also described a specific vulnerability as something that "could potentially" allow an attacker to compromise information, when in fact the vulnerability had already been utilized to do so on at least three occasions.[4]

In recent comment letters, the SEC has increasingly asked companies that have experienced a cyber attack to revise risk factor disclosure to be clear that a cyber-attack has, in fact, occurred – rather than framing an attack as a hypothetical (i.e. "We *may* experience cyber-attacks").[5] SEC comments have also asked companies to consider disclosure on how the "board administers its risk oversight function in overseeing cybersecurity risks," including in the context of companies that had experienced a cyber breach and failed to adequately disclose this fact. [6] Board oversight disclosure is now required under the new cybersecurity disclosure rules, and companies should be mindful that the SEC may be focused on how this disclosure ties into its risk factor discussion.

2. Artificial Intelligence ("AI")

The use of AI technologies continues to evolve, and companies are increasingly considering the means and the extent to which AI will be used in their operations. While AI technologies offer significant opportunities, they also pose significant, complex and novel risks, especially during early developmental stages of the technology. Risks related to AI range from operational risks such as the potential for factual errors or inaccuracies in work product developed with AI, distribution of confidential information using AI technologies, ethical risks related to the potential for inherent biases in the algorithm or programming, privacy concerns with respect to data dissemination or security issues, risks related to intellectual property rights with respect to both the inputs to the program and ownership rights to AI work product, and risks related to AI's impact on the workforce, among others. Cybersecurity-related issues are also a significant risk for AI. As the SEC's Corp Fin Director Erik Gerding noted, "artificial intelligence and other technologies may enhance both the ability of public companies to defend against cybersecurity threats but also the capacity of threat actors to launch sophisticated attacks."

Statements from the SEC have underscored the increasing importance of accurate AI disclosure. Notably, Chair Gary Gensler cautioned companies in early December not to "AI wash," or mislead investors as to their true artificial intelligence capabilities. Risk factors can play a crucial role in achieving this, and companies should accurately address risks related to their use of AI technologies and have a reasonable basis for claims they make about AI. As the SEC's Corp Fin Director Erik Gerding explained, risk factor disclosure on AI should be "particularized to the facts and circumstances" of a given company, including how AI could impact the market for that company's goods and services. In assessing whether AI should be addressed in risk factors, companies should consider their disclosure on AI across their annual report, website, press releases and other public

---

3 The 2018 guidance specifically noted that it would be "helpful for companies to consider the following issues, among others, in evaluating cybersecurity risk factor disclosure" including "the aspects of the company's business and operations that give rise to material cybersecurity risks and the potential costs and consequences of such risks." *See* page 13 at Commission Statement and Guidance on Public Company Cybersecurity Disclosures. Companies may also want to consider the December 2019 guidance from the SEC focused on risks related to the potential theft or compromise of their technology, data, or intellectual property in connection with their international operations.

4 The Company also stated that it was both "still investigating" and had hired third-party cybersecurity experts to assist in an investigation of "whether a vulnerability in the Orion monitoring products was exploited" when it already knew that the vulnerability had been exploited on at least three prior occasions. Complaint, SEC v. SolarWinds Corp. and Brown, No. 1:23-cv-9518 (S.D.N.Y. Oct. 30, 2023). Also, *see* our alerts, "Time to Revisit Risk Factors in Periodic Reports" and "SEC Fines Yahoo $35 Million for Failure to Timely Disclose Cyber Breach."

5 For example, "In light of the data breach, please update this risk factor language that characterizes that risk as potential or hypothetical to note that you have experienced a data breach and describe it as necessary. Additionally, please tell us whether you believe this data breach was material and explain how you reached this conclusion." Comment letter to Altair Engineering, Inc. on its Form 10-Q (June 12, 2023).

6 Comment letter to Altair Engineering, Inc. (June 12, 2023). *See also,* comment letter to Newtekone, Inc. on its (February 23, 2023).

statements, and determine whether risks related to AI should be disclosed as a material risk to their businesses and prospects.

3. Macroeconomic Considerations: Uncertainty, Interest Rates and Inflation

Economic uncertainty and volatility, including as a result of high interest rates and inflation, continued through much of 2023, but more recently economists, including Treasury Secretary Janet Yellen, have predicted a "soft landing" in which "the economy continues to grow, the labor market remains strong and inflation comes down."[7] Similarly, the Congressional Budget Office has predicted slightly increased unemployment levels and an ultimate decline in inflation in 2024.[8] In light of these recent updates to the economic forecast, companies may need to also change their approach to risk factor disclosure related to the economy. For example, companies may want to consider disclosure on their approach to cost-saving measures, including headcount and discretionary expenses, while referencing moderately improved economic conditions in areas such as capital formation or demand from consumers.

Additionally, companies should consider whether they need to update risk factor disclosure related to inflation and interest rates, including their impact on revenues or earnings. While the Federal Reserve has recently held interest rates steady, rates currently remain at a multi-decade high level. The Federal Reserve has indicated likely interest rates cuts in 2024,[9] but companies should still carefully consider the risks they face should there be ongoing inflation and high interest rates, which can include increased operating costs, such as fuel and energy, transportation and shipping, materials, and wages and labor costs. Additionally, elevated interest rates impact companies by increasing the cost of debt and limiting options to refinance existing debt on favorable terms or at all.[10]

Further, while the Federal Reserve's recent announcements are being positively viewed by the market, the equity capital markets continue to be volatile, which may adversely affect a company's financial condition. This volatility could impact a company's plans for growth or its ability to access the capital markets to raise funds, either for general corporate purposes or as consideration for mergers and acquisitions. A company should assess any material risks related to these developments and whether they should be disclosed in its risk factors.

4. International Geopolitics

Conflicts and instability across the globe may pose material risks to companies and their businesses, including through fluctuations in commodity prices and changes in the availability and cost of supplies and energy. Companies with significant operations or investments in impacted regions should evaluate risks related to ongoing conflicts and consider updating their risk factor disclosure accordingly. It is imperative that companies tailor these risks to their particular situation and operations.

In May 2022, the SEC posted a sample comment letter to companies emphasizing their potential disclosure obligations related to direct or indirect impacts that Russia's actions in Ukraine and the international response have or may have on their business, which can provide guidance to companies thinking about potential disclosure updates with respect to other global conflicts that might impact their businesses. In its sample comment letter, the SEC specifically noted that, to the extent material, companies should provide detailed disclosure regarding risks related to actual or potential disruptions in supply chains and new or heightened risks of potential cyberattacks by state actors. Similarly, companies may want to consider updates related to global supply chain risks, including in light of recent attacks on merchant ships in the Red Sea that have led shipping companies to avoid the region and could result in increased shipping costs that impact companies.

In July 2023, the SEC also issued a sample comment letter related to risks for companies with operations in China. With respect to risk factor disclosure, the Staff noted it has been continuing to issue comments seeking more "specific and prominent disclosure about material risks related to the role of the government of the People's

---

7 *See* "Yellen Says Economy on Path to Soft Landing," Wall Street Journal (December 12, 2023).

8 *See* "Congressional Budget Office projection sees higher unemployment, inflation just over 2% next year", Fortune (December 15, 2023).

9 *See* "With rate hikes likely done, Fed turns to timing of cuts," Reuters (December 13, 2023).

10 For more information, see our prior alert, "Inflation and increasing interest rates reshape US leveraged finance markets."

Republic of China in the operations of China-based companies."[11] To the extent that companies have operations in China, they should take into account the sample comment letter, as well as recent developments in the region, while preparing their risk factor disclosure.

In light of increased geopolitical tension in the world, companies should also consider risks related to sanctions imposed on any countries in which they have business relationships or in which they do business.[12] For example, sanctions have recently been imposed against third-country suppliers and networks that materially support Russia's war in Ukraine.[13] As a result of sanctions, potential risks can also include supply chain disruptions, contractual disputes and litigation, asset freezes, disruptions in or interferences with business continuity, capital restrictions, countersanctions, heightened cybersecurity concerns, changes to customer demand and reputational risks, among others. As in call cases, it is important that impacted companies accurately describe the risks that apply to their particular facts and circumstances.

5. Climate

Climate change issues remain an area of focus for companies, investors and the SEC. Notably, considerations around climate disclosures have become more nuanced as institutional investors and companies have reassessed their approach to ESG and refocused on the importance of shareholder value.[14] Greenhushing, where companies deliberately downplay their ESG initiatives to reduce public scrutiny, appears on the rise, in part due to "greenwashing" accusations and liability concerns over public statements relating to ESG.

The SEC continues to scrutinize companies' climate-related disclosures. The SEC's proposed climate change rules – whose adoption has been delayed from October 2023 to April 2024 according to the SEC's recent Reg Flex agenda[15] – would require registrants to provide detailed climate-related disclosures in registration statements and periodic reports filed with the SEC, including disclosure of greenhouse gas emissions and extensive discussion of climate-related risks that are reasonably likely to have a material impact on the business. While the climate change disclosure rules remain in proposed form, the SEC has continued to issue climate related comments on Form 10-K and 20-F filings in 2023, which mirror those included in the SEC's 2021 sample comment letter to companies. These comments predominantly focused on inquiries regarding "the physical effects of climate change on…operations and results"[16] and asking for additional disclosure on "the indirect consequences of climate-related regulation and trends."[17]

---

11 The sample comment letter included the following sample comment related to risk factor disclosure: "Given the significant oversight and discretion of the government of the People's Republic of China (PRC) over the operations of your business, please describe any material impact that intervention or control by the PRC government has or may have on your business or on the value of your securities. We remind you that, pursuant to federal securities rules, the term 'control' (including the terms 'controlling,' 'controlled by,' and 'under common control with') means 'the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a person, whether through the ownership of voting securities, by contract, or otherwise.'"

12 *See, e.g.,* our prior alert, "Taiwanese companies in a world of "clubs" and "fences.""

13 *See* the U.S. Department of the Treasury's press release, "Treasury Imposes Sanctions on More Than 150 Individuals and Entities Supplying Russia's Military-Industrial Base," (December 12, 2023).

14 See, for example, "Are Recent Adjustments in the ESG Universe A Retreat?", Forbes (August 31,2023).

15 For more information, *see* our alert, "SEC Proposes Long-Awaited Climate Change Disclosure Rules."

16 For example, "Please discuss the physical effects of climate change on your operations and results. This disclosure may include the following: severity of weather, such as floods, hurricanes, sea levels, arability of farmland, extreme fires and water availability and quantity; quantification of material weather-related damages to your property or operations; potential for indirect weather-related impacts that have affected or may affect your major customers or suppliers; decreased agricultural production capacity of your customers in areas affected by drought or other weather-related changes; and any weather-related impacts on the cost or availability of insurances. Your response should include quantitative information for each of the periods covered by your Form 10-K and explain whether increased amounts are expected in future periods." Comment letter to Beyond, Inc. on its Form 10-K (September 19, 2023).

17 For example, "To the extent material, discuss the indirect consequences of climate-related regulation or business trends, such as the following: decreased demand for goods or services that produce significant greenhouse gas emission or are related to carbon-based energy sources; increased demand for goods that result in lower emissions than competing products; increased competition to develop innovative new products that result in lower emissions; increased demand for generation and transmission of energy from alternative energy sources; and any anticipated reputational risks resulting from operations or products that produce material greenhouse gas emissions." Comment letter to Ferroglobe PLC on its Form 10-F (August 24, 2023). *See also, e.g.,* comment letter to OKTA, Inc. on its Form 10-K (September 14, 2023).

In addition, there are increasing disclosure and other compliance requirements for companies doing business in certain regions that could potentially impact a company's risk factor disclosure. For example, companies that do business in California should consider the potential effects of recently adopted CA legislation,[18] which includes novel disclosure requirements related to voluntary carbon offsets and a wide range of environmental marketing claims, and whether any risks related to such laws should be disclosed. Similarly, any companies that generate substantial revenues from within the EU should be considering the applicability of the Corporate Sustainability Reporting Directive ("CSRD"), which will require companies to make detailed disclosures in relation to a range of sustainability-related issues, including climate change.[19] Companies should consider whether the additional disclosures necessitated by climate-related regulations require corresponding risk factor disclosures related to regulatory developments.

Further, companies should consider potential impacts of the Inflation Reduction Act of 2022, which provides tax credits and other federal incentives designed to encourage investments in clean energy, such as large-scale clean power generation carbon capture and storage projects underway in Texas. Finally, on an international scale, at the UN Climate Change Conference, COP28, negotiators agreed to "ratchet up climate action…with the overarching aim to keep the global temperature limit of 1.5°C within reach." The agreement calls on parties to take actions towards "achieving a tripling of renewable energy capacity and doubling energy efficiency improvements by 2030… [by] accelerating efforts towards the phase-down of unabated coal power, phasing out inefficient fossil fuel subsidies, and other measures that drive the transition away from fossil fuels in energy systems."[20]

Given these at times competing considerations, companies should carefully assess their risk factor disclosure related to climate, including (1) whether pending regulatory requirements or developments in the area of climate or sustainability pose any material risks or challenges to their business, (2) whether any material risks related to their climate goals and commitments are appropriately disclosed, and (3) whether any of the climate information contained in their sustainability reports is or has become material and therefore required to be included in their Form 10-K/20-F.[21]

6. Internal Controls

A company's internal control over financial reporting is the foundation on which the accuracy of its financial reporting depends, and it is important that risks related to internal controls are properly evaluated and disclosed. According to an Audit Analytics report, 68% of financial restatements resulted in a negative income impact during 2022.[22] While the accuracy of financial statements is always crucial, the SEC's new clawback rules put a new spotlight on internal controls by requiring companies to recoup any incentive-based compensation that was erroneously awarded to executive officers based on a financial statement error that requires either a little "r" or big "R" restatement.

In addition, risks related to failures in disclosure controls and procedures have gained increased scrutiny in recent months, as an increasing number of SEC statements and enforcement actions have focused on failures in these controls. For example, in February 2023 the SEC charged Activision Blizzard Inc.[23] with a failure to maintain disclosure controls and procedures necessary to collect and analyze employee complaints of workplace

---

18 Specifically, Senate Bill 253, the Climate Corporate Data Accountability Act, Senate Bill 261, Greenhouse Gases: Climate-Related Financial Risk and Assembly Bill 1305, the Voluntary Carbon Market Disclosures Act.

19 The new law applies to both large EU-domiciled entities *and* to non-EU entities which generate substantial revenues from within the EU, as well as entities with debt and equity securities listed on EU regulated markets. Effective January 5, 2023, the CSRD will apply to in-scope companies progressively from 2024 to 2028, depending on size and domicile.

20 The UN's press release is available here.

21 For example: "We note that you provided more expansive disclosure in your Fiscal 2022 Social Impact and Sustainability Report ("SIS Report") and Climate Transition Plan 2022 ("CT Plan") than you provided in your SEC filings. Please advise us what consideration you gave to providing the same type of climate-related disclosure in your SEC filings as you provided in your SIS Report and CT Plan." Comment letter to Estee Lauder Companies Inc. on its Form 10-K (September 14, 2023).

22 The report is available here.

23 The SEC's order is available here.

misconduct across separate business units[24] and in November 2023, the SEC charged Charter Communications[25] Inc. for failure to establish internal accounting controls to provide reasonable assurances that its trading plans were conducted in accordance with the board of directors' authorization, which required the use of trading plans in conformity with Rule 10b5-1.[26]

In light of the potential risks and increased regulatory scrutiny over a company's controls this year, companies should consider any material risks related to potential failures in internal controls, which can range from language addressing the risk of material weaknesses and restatements, to a broader scope addressing legal and regulatory risks from potential failures in maintaining adequate controls.

Part II: Four Important Drafting Considerations when Updating Annual Memo Risk Factor Disclosures

1. Avoid Boilerplate Disclosures

The SEC has long emphasized that companies should tailor their risk factor disclosure to their particular facts and circumstances, and avoid generic and boilerplate disclosure, in compliance with Item 503(c) of Regulation S-K, which explicitly directs companies to "not present risks that could apply to any issuer or any offering." Recent SEC comment letters reflect this focus, asking companies to "place risk factors in context so your reader can understand the specific risks as it applies to you", avoid "overly broad and boilerplate disclosure and provide more specific information to focus on actual risks" and "particularize to your company or delete those risk factors that do not comply with these requirements and prohibitions." At a recent speech, Director Erik Gerding underscored this point, noting that boilerplate risk factors are not helpful to investors, who benefit much more from a sense of how risks apply to a particular issuer.[27]

2. Carefully Scrutinize Hypothetical Statements

It is imperative that any hypothetical statements in risk factor disclosures (e.g., the statements that an event "could" or "may" occur rather than "has" or "did" occur in the past) are carefully scrutinized and evaluated. The SEC continues to focus on this topic and has instituted enforcement actions against many companies for disclosures regarding hypothetical risks which have already occurred.[28] In addition to the risk of enforcement action, shareholders have filed claims under Section 10(b) of the Securities Exchange Act of 1934, as amended, alleging that statements in a company's risk factors were materially misleading because a company stated that an event only "may" or "could" occur, when the event was no longer hypothetical at the time of the disclosure. Companies should conduct a careful review any hypothetical risk factor language and clarify whether a potential disclosed risk has in fact occurred to some degree.[29]

3. Review for Internal Consistency

When drafting or reviewing risk factors, companies should review for consistency against other sections of their annual report, as risk factors should not be drafted in a vacuum. This includes looking at the Business and MD&A sections (i.e., for foreign private issuers, the equivalents of Items 4 and 5 of Form 20-F) and the financial

---

24 Specifically, the SEC criticized the company for not including information about employee complaints or reported incidents of workplace misconduct among the information that was required to be reported to the company's disclosure committee. As a result, management did not have sufficient information about the volume and substance of employee complaints to assess the related risks, whether material issues existed that warranted disclosure to investors, or whether the disclosures it made to investors in connection with these risks were sufficient and not misleading.

25 The SEC's order is available here.

26 According to the SEC, many of the company's trading plans allowed for increases to the amount of share repurchases if the company opted to conduct certain debt offerings, which effectively gave the company the ability to increase trading activity after adoption of its trading plans, in violation of Rule 10b5-1 and, as a result, the board's authorization. The SEC order found that "the company did not have reasonably designed controls to analyze whether the discretionary element of the accordion provisions was consistent with the [b]oard's authorizations."

27 See "Remarks at the Practicing Law Institute's 55th Annual Institute on Securities Regulation."

28 Refer to Part I, Item 1. Cybersecurity, of this client alert, regarding the SolarWinds SEC enforcement action.

29 Disclosure may be required whether or not the degree of occurrence is material on its own. For more information, see our prior alert, "Time to Revisit Risk Factors in Periodic Reports."

statements to confirm that any key factors, changes and liabilities are considered, if appropriate. Companies should also consider their budgeting plans and risks related to achieving their business goals in drafting risk factors. It is often appropriate to provide cross-references to other sections of the annual report (e.g., the new cybersecurity risk management disclosures to the cybersecurity risk factors); however, any material risks should be disclosed in the risk factor section as well.

4. Remember to Update or Delete Risk Factors That Have Changed in Importance or Are No Longer Relevant

When considering risk factor disclosure, it is important not only to update for newly-realized risks, but to confirm that all risks disclosed remain material and relevant, and to remove, update or revise those that no longer present material risks to the company or those for which the potential impact on the company has changed materially. Updates for risk factors should be considered through the filing date of the annual report, rather than at the end of the fiscal period covered by the report. For example, in May 2023, the Federal Public Health Emergency Declaration issued in response to COVID-19 was lifted by the federal government. Companies should consider to what extent, if any, the ongoing COVID-19 endemic impacts their business, and may determine to eliminate altogether or significantly streamline any COVID-19 specific risk factor disclosures.

5. Reminders on the Risk Factor Presentation:

- **Ordering of Risks**. Although risks are not required to be ordered by magnitude of importance or potential impact, it is generally considered a best practice to do so. Item 105 of Regulation S-K does state that risks should be "organized logically," and Item 3.B of Form 20-F states that "[c]ompanies are encouraged, but not required, to list the risk factors in the order of their priority to the company," so companies should consider the order that makes the most sense for investors. In addition, companies are required to organize risk factors into groups of related risk factors under "relevant headings" and provide sub-captions for each risk factor (while this is not technically required for foreign private issuers, they routinely do this in their Form 20-Fs). Further, risk factors should be specific to the company or its industry. For any risk factors that apply generically to any registrant or offering and are not tailored, the company must disclose the generic risk factors at the end of the risk factor section under the caption "General Risk Factors" (again while this is not technically required for foreign private issuers, they routinely do this in their Form 20-Fs). These requirements have been in effect since 2020, and companies should annually review their groupings and headings to confirm any updates or changes to their risk factor section's organization.

- **Risk Factor Summaries**. If your risk factor section exceeds 15 pages, you must include a series of concise, bulleted, or numbered statements that is no more than two pages summarizing the principal risk factors and place this summary at the "forepart" or beginning of the Form 10-K. This can be combined with your forward-looking statement legend to avoid repetition, and companies may consider this approach so long as the legend is appropriately titled to reflect its dual purposes (i.e., "Cautionary Note Regarding Forward-Looking Statements and Risk Factor Summary"). This is not technically required for Form 20-F, although some foreign private issuers may decide to do so in order to self-present more closely to domestic issuers.

Conclusion

In light of upcoming annual report deadlines for calendar year-end companies, companies should start their Form 10-K/20-F processes by reviewing and updating their risk factors early on, including by assessing the material risks that impact their businesses. Well-drafted risk factors play a crucial role in defending public companies against allegations of fraud under the U.S. federal securities laws, and companies should therefore take the time to update their disclosure for new material risks and tailor risk factor disclosure to their own facts and circumstances.

The following White & Case attorneys authored this alert:

Maia Gez
Scott Levi
Melinda Anderson
Danielle Herrick
Taylor Pullins
Hope Anderson
Cristina Brayton-Lewis
Chad Klitzman

White & Case Team Members:

A.J. Ericksen: 713-496-9688, aj.ericksen@whitecase.com
Colin J. Diamond: 212-819-8754, cdiamond@whitecase.com
Elodie Gal: 212-819-8242, egal@whitecase.com
Maia Gez: 212-819-8217, maia.gez@whitecase.com
David Johansen: 212-819-8509, djohansen@whitecase.com
Scott Levi: 212-819-8329, scott.levi@whitecase.com
Daniel Nussen: 213-620-7796, daniel.nussen@whitecase.com
Kimberly Petillo-Decossard: 212-819-8398, kimberly.petillo-decossard@whitecase.com
Taylor Pullins: 713-496-9653, taylor.pullins@whitecase.com
Jonathan Rochwarger: 212-819-7643, jrochwarger@whitecase.com
Joel Rubinstein: 212-819-7642, joel.rubinstein@whitecase.com
Michelle Rutta: 212-819-7864, mrutta@whitecase.com
Elliott Smith: 212-819-7644, elliott.smith@whitecase.com
Melinda Anderson: 212-819-7002, melinda.anderson@whitecase.com
Danielle Herrick: 212-819-8232, danielle.herrrick@whitecase.com
Patti Marks: 212-819-7019, pmarks@whitecase.com
Sarah Hernandez: 212-819-8429, sarah.hernandez@whitecase.com