

Expect Sweeping Changes to the SEC Next Year: An Insider's Preview Briefing Materials

Table of Contents

- **Four Years of Evolving Form 10-K Human Capital Disclosures**
- **Webcast: IPO and Public Company Readiness: Advance Planning for 2025 and 2026 IPOs – Corporate Governance and ESG Considerations**
- **SEC Desktop Calendar for 2025**
- **Fifth Circuit Finds SEC’s “About-Face” On Proxy-Firm Disclosure Rule Arbitrary And Capricious**
- **Early Insights from Insider Trading Policies Filed by S&P 500 Companies under the SEC’s New Exhibit Requirement**
- **SEC Adopts Sweeping New Climate Disclosure Requirements for Public Companies**
- **Shareholder Proposal Developments During the 2024 Proxy Season**
- **Considerations for Preparing Your 2023 Form 10-K**
- **SEC Successfully Prosecutes Novel “Shadow Trading” Theory at Trial**
- **Webcast: SEC Enforcement Update**
- **Securities Enforcement 2024 Mid-Year Update**
- **Gibson Dunn Environmental, Social and Governance Update**
- **U.S. Cybersecurity and Data Privacy Review and Outlook – 2024**
- **Dismissal of Much of SEC’s SolarWinds Complaint Has Potentially Broad Implications for SEC Cybersecurity Enforcement**
- **Cybersecurity Overview: A Survey of Form 10-K Cybersecurity Disclosures by the S&P 100 Companies**

GIBSON DUNN



Securities Regulation & Corporate Governance
and Labor & Employment Update

December 16, 2024

Four Years of Evolving Form 10-K Human Capital Disclosures

A Survey of Disclosures from the S&P 100 During the Four Years Following Adoption of the Securities and Exchange Commission Rule.

Human capital resource disclosures by public companies have continued to be a focus since the U.S. Securities and Exchange Commission (the “Commission”) adopted the new rules in 2020, not only for companies making the disclosures, but employees, investors, and other stakeholders reading them. This alert updates the alert we issued in November 2023, “*Form 10-K Human Capital Disclosures Continue to Evolve*,” available [here](#), and reviews disclosure trends among S&P 100 companies categorized into 28 topic areas. Each of these companies has now included human capital disclosure in their past four annual reports on Form 10-K. This alert also provides practical considerations for companies as we head into 2025.

Overall, our findings indicate that companies are generally making only minor changes to their disclosures year over year, and these minor changes generally included shortening of company disclosures, maintaining or decreasing the number of topics covered, and including slightly less quantitative information in some areas.^[1] Specifically, we identified the following trends regarding the S&P 100 companies’ human capital disclosures compared to the previous year:

- **Length of disclosure.** Fifty-seven percent of surveyed companies decreased the length of their disclosures, 34% increased the length of their disclosures, and the length of the remaining 9% remained the same.

- *Number of topics covered.* Forty-one percent of surveyed companies decreased the number of topics covered, 13% increased the number of topics covered, and the remaining 46% covered the same number of topics.
- *Breadth of topics covered.* Across all companies, the prevalence of 10 topics increased, nine topics decreased, and nine topics remained the same.
 - The most significant year-over-year increases in frequency involved Culture Initiatives (30% to 35%) and Pay Equity (48% to 50%) disclosures.
 - The most significant year-over-year decrease involved COVID-19 disclosures, which declined in frequency from 34% to 1%. Other year-over-year decreases related to disclosures addressing Diversity Targets and Goals (21% to 14%), Diversity in Promotion (29% to 26%), Quantitative Diversity Statistics regarding Gender (63% to 60%), and Community Investment (28% to 25%).
- *Most common topics covered.* This year, the topics most commonly discussed generally remained consistent with the previous two years. For example, Talent Development, Diversity and Inclusion, Talent Attraction and Retention, Employee Compensation and Benefits, and Monitoring Culture remained the five most frequently discussed topics. The topics least discussed this most recent year, however, changed slightly from that of the previous year as COVID-19 disclosures, and Diversity Targets and Goals dropped into the five least frequently covered topics.
- *Industry trends.* Within the technology and finance industries, the trends that we saw in the previous year regarding the frequency of topics disclosed generally remained the same.

I. Background on the Requirements

As we previously discussed in our client alert titled “Discussing Human Capital: A Survey of the S&P 500’s Compliance with the New SEC Disclosure Requirement One Year After Adoption,” available [here](#), on August 26, 2020, the Commission voted three-to-two to approve amendments to Items 101, 103, and 105 of Regulation S-K, including the principles-based requirement to discuss a registrant’s human capital resources to the extent material to an understanding of the registrant’s business taken as a whole.^[2] Specifically, public companies’ human capital disclosure must include “the number of persons employed by the registrant, and any human capital measures or objectives that the registrant focuses on in managing the business (such as, depending on the nature of the registrant’s business and workforce, measures or objectives that address the development, attraction, and retention of personnel).”

Notably, since 2021 the Commission’s agenda list has included new human capital disclosure rules that were expected to be more prescriptive than the current rules,^[3] in part, because one of the main criticisms of the existing human capital rules is lack of comparability across companies. The future of these rules is even less clear now as Chair Gensler who pushed for these rules (along with other rules, such as climate change) announced that he will be leaving the SEC in January 2025 in light of the new incoming administration. In the meantime, as our survey demonstrates, while company human capital disclosures vary—which is expected under the

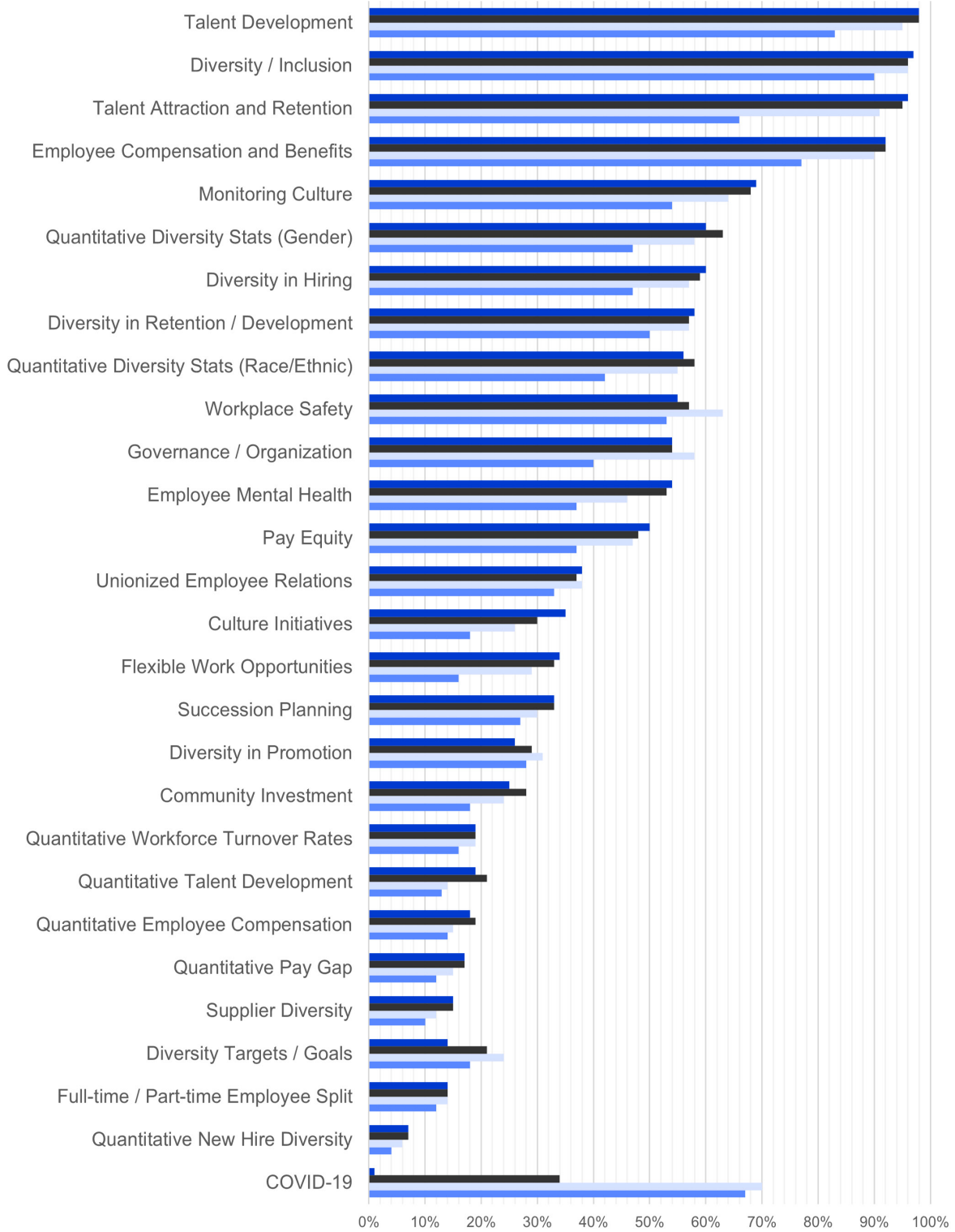
principles-based regime—comparability across the disclosures exists. The next four sections show the relevant data from our survey.[\[4\]](#)

II. Disclosure Topics

Our survey classifies human capital disclosures into 28 topics, each of which is listed in the following chart, along with the number of companies that discussed the topic in each of 2021, 2022, 2023, and 2024. Each topic is described more fully in the sections following the chart.

Human Capital Disclosures

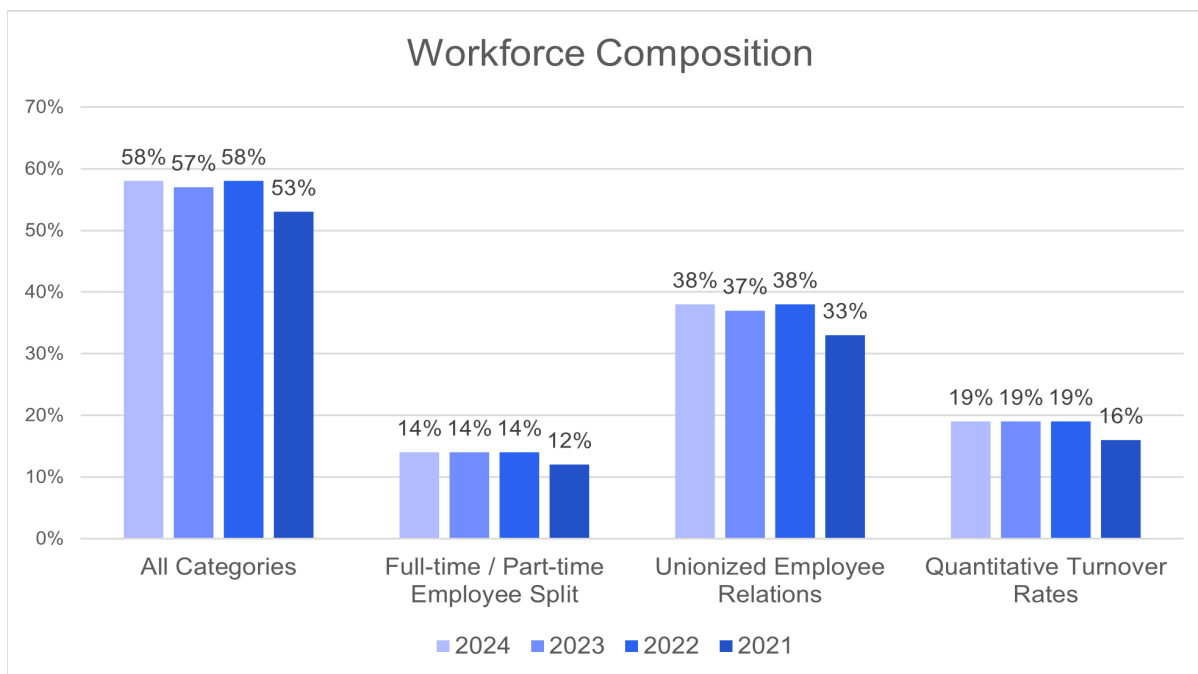
■ 2024 ■ 2023 ■ 2022 ■ 2021



A. Workforce Composition

Among S&P 100 companies, 58% included disclosures relating to workforce composition in one or more of the following categories:

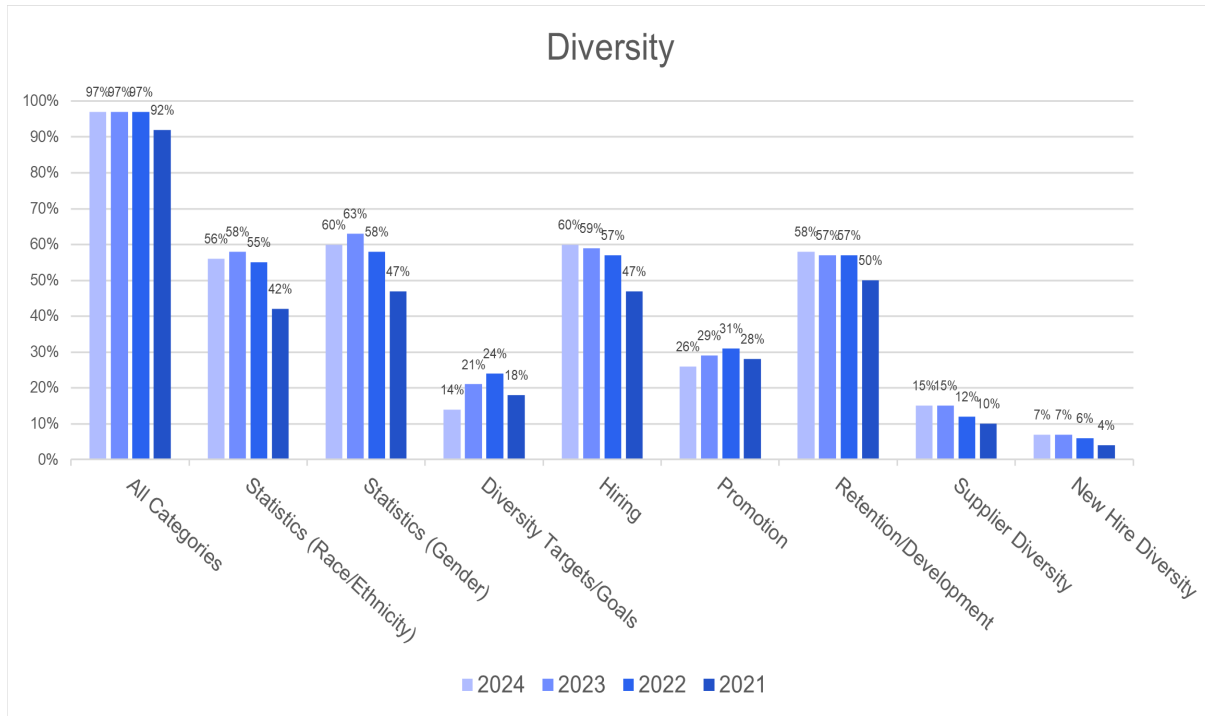
- **Full-time/part-time employee split.** While most companies provided the total number of full-time employees, only 14% of the companies surveyed included a quantitative breakdown of the number of full-time versus part-time employees or salaried versus hourly employees, consistent with the previous two years. Similarly, 66% of companies provided statistics on the number of seasonal employees and/or independent contractors or a breakdown of employees by business segment, job function, or geographical location, the same as the previous year, and up from and 60% in 2021.
- **Unionized employee relations.** Of the companies surveyed, 38% stated that some portion of their workforce was part of a union, works council, or similar collective bargaining agreement.^[5] These disclosures generally included a statement providing the company's opinion on the quality of labor relations, and in many cases, disclosed the number of unionized employees.
- **Quantitative workforce turnover rates.** Although a majority of companies discussed employee turnover and the related topics of talent attraction and retention in a qualitative way (as discussed in Section II.B. below), only 19% of companies surveyed provided specific employee turnover rates (whether voluntary or involuntary), consistent with the previous two years.



B. Diversity

Among S&P 100 companies, 97% included disclosures relating to diversity in one or more of the following categories:

- **Diversity and inclusion.** This was the most common diversity-related disclosure topic, with 97% of companies including a qualitative discussion regarding the company's commitment to diversity, equity, and inclusion ("DEI"), consistent with the previous two years and up slightly from 91% in 2021. The depth of these disclosures varied, ranging from generic statements expressing the company's support of diversity in the workforce to detailed examples of actions taken to recruit and support underrepresented groups and increase the diversity of the company's workforce.
- **Priorities within diversity.** Companies disclosed different areas of focus for diversity efforts and programming within the organization. The most common disclosure was diversity in the company's hiring practices (60% of companies in 2024, up dramatically from 47% in 2021), followed by diversity in the retention or development of the company's current workforce (58% of companies in 2024, up slightly from 50% in 2021), diversity in the company's promotion practices (26% of companies in 2024, down from a high of 31% in 2022), and finally diversity in the company's suppliers (15% of companies in 2024, up slightly from 10% in 2021). A decreasing minority of companies also discussed, in qualitative or quantitative terms, the companies' commitments to aspirational diversity goals or targets (14% of companies in 2024, down from a high of 24% of companies in 2022), with such decrease likely due to the heightened legal risk associated with DEI programs following the June 2023 United States Supreme Court decision in *Students for Fair Admissions v. Harvard*.
- **Quantitative diversity statistics.** Many companies also included a quantitative breakdown of the gender or racial representation of the company's workforce: 60% included statistics on gender and 56% included statistics on race or ethnicity (down slightly compared to 2023, but up significantly from 47% and 42%, respectively, in 2021). Companies generally provided gender statistics on both a global and U.S. basis, whereas nearly all companies provided race or ethnicity statistics for their U.S. workforce only. Most companies provided these statistics in relation to their workforce generally, regardless of position; however, an increased subset (40% in 2024, compared to 25% in 2021) included separate statistics for different classes of employees (e.g., managerial, vice president and above, etc.). Similarly, 12% of companies also provided separate statistics for their boards of directors (compared to 10% in each of 2023 and 2022 and 4% in 2021). Some companies also included numerical goals for gender or racial representation, either in terms of overall representation, promotions, or hiring—11% of companies included these diversity goals or targets (compared to 15% in 2023, 18% in 2022, and 14% in 2021).



C. Recruiting, Training, Succession

Among S&P 100 companies, 99% included disclosures relating to talent and succession planning in one or more of the following categories:

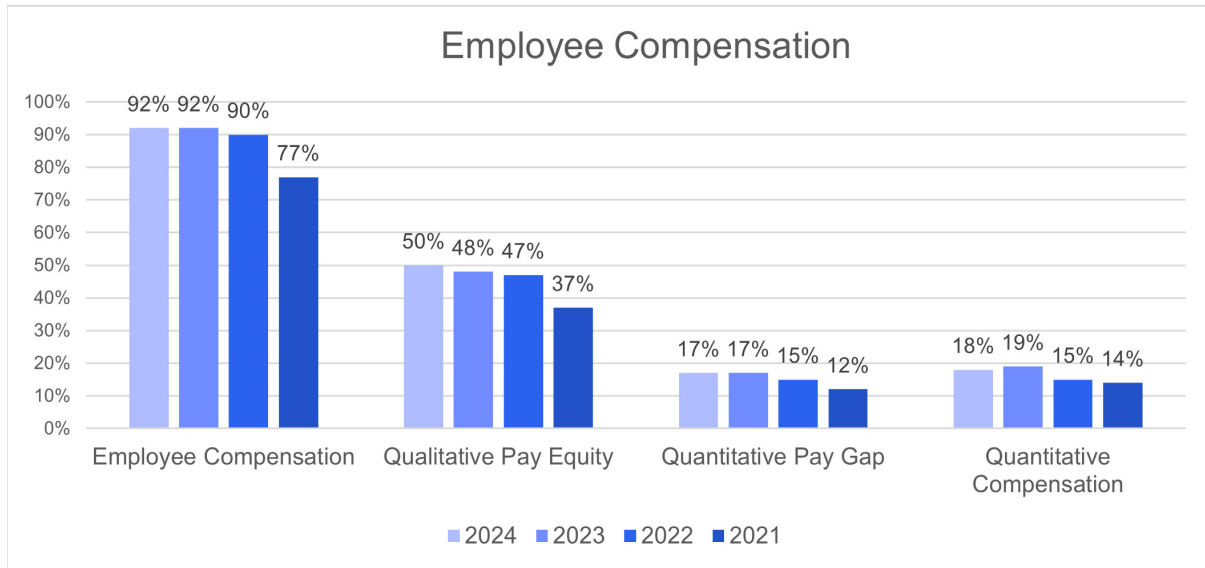
- Talent attraction and retention.** These disclosures were generally qualitative and focused on efforts to recruit and retain qualified individuals. While general statements regarding recruiting and retaining talent were very common, with 96% of companies including this type of disclosure (relatively flat in the prior two years, but up significantly from 66% in 2021), quantitative measures of retention, like workforce turnover rate, were uncommon, with only 19% of companies disclosing such statistics (as noted above).
- Talent development.** Disclosures related to talent development were the most common category, with 98% of companies including a qualitative discussion regarding employee training, learning, and development opportunities, up from 83% in 2021. This disclosure tended to focus on the workforce as a whole rather than specifically on senior management. Companies generally discussed training programs such as in-person and online courses, leadership development programs, mentoring opportunities, tuition assistance, and conferences. Some companies discussed quantitative figures related to talent development, such as the number of hours employees spent on learning and development or the company's investment in development resources, with 19% of companies including this type of disclosure.
- Succession planning.** Only 33% of companies surveyed addressed their succession planning efforts, which may be a function of succession being a focus area primarily for executives rather than the human capital resources of a company more

broadly. However, this is up from 27% of companies who discussed succession planning in 2021.



D. Employee Compensation^[6]

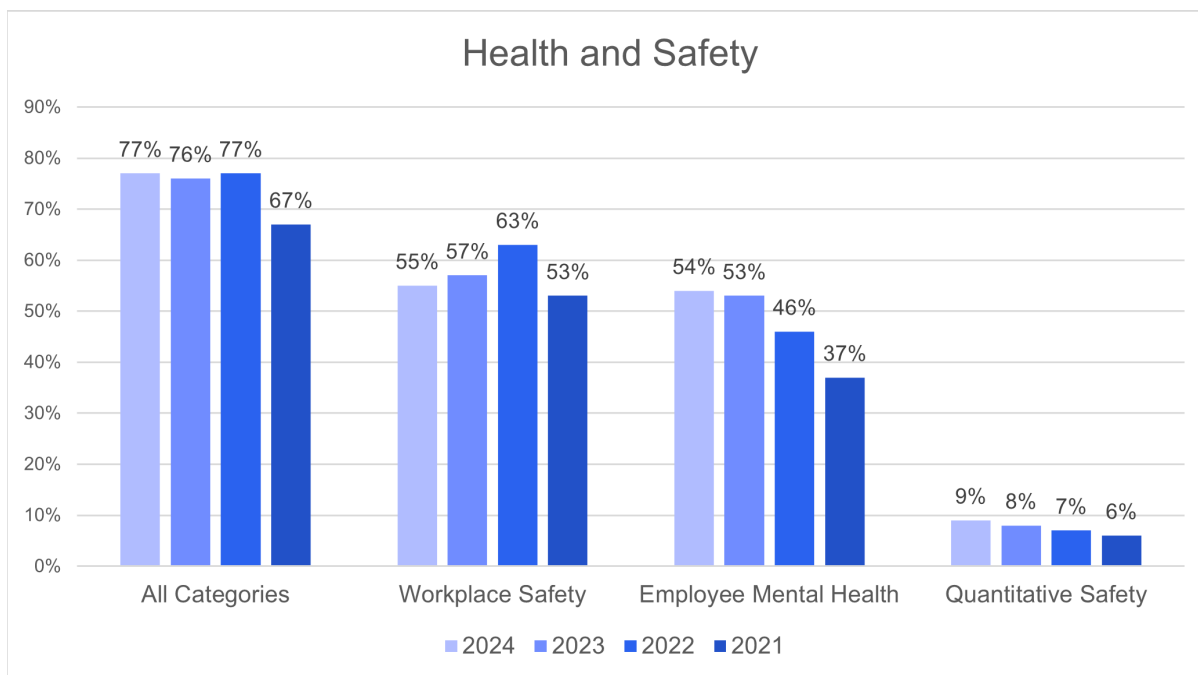
Among S&P 100 companies, 92% included disclosures relating to employee compensation, up from 77% in 2021. All of those companies included a qualitative description of the compensation and/or benefits program offered to employees, with a small minority providing quantitative measures such as minimum or average wages or investment in benefits (17% of companies surveyed in 2024, up from 12% in 2021). Of the companies surveyed, 50% addressed pay equity practices or assessments (up from 37% in 2021), and substantially fewer companies included quantitative measures of the pay gap between racially or ethnically diverse and nondiverse employees or male and female employees (17% of companies surveyed in 2024, up from 12% in 2021).



E. Health and Safety

Among S&P 100 companies, 77% included disclosures relating to health and safety in one or both of the following categories:

- Workplace safety.** Of the companies surveyed, 55% included qualitative disclosures relating to workplace health and safety, down from 63% in 2022, typically consisting of statements about the company's commitment to safety in the workplace generally and compliance with applicable regulatory and legal requirements. However, 9% of companies surveyed provided quantitative disclosures in this category, generally focusing on historical and/or target incident or safety rates or investments in safety programs. These quantitative disclosures tended to be more prevalent among industrial, energy, and manufacturing companies.
- Employee mental health.** In connection with disclosures about benefits provided to employees, including benefits intended to support employees' general wellness or wellbeing, 54% of companies disclosed initiatives taken to support employees' mental or emotional health and wellbeing, up from 37% in 2021.

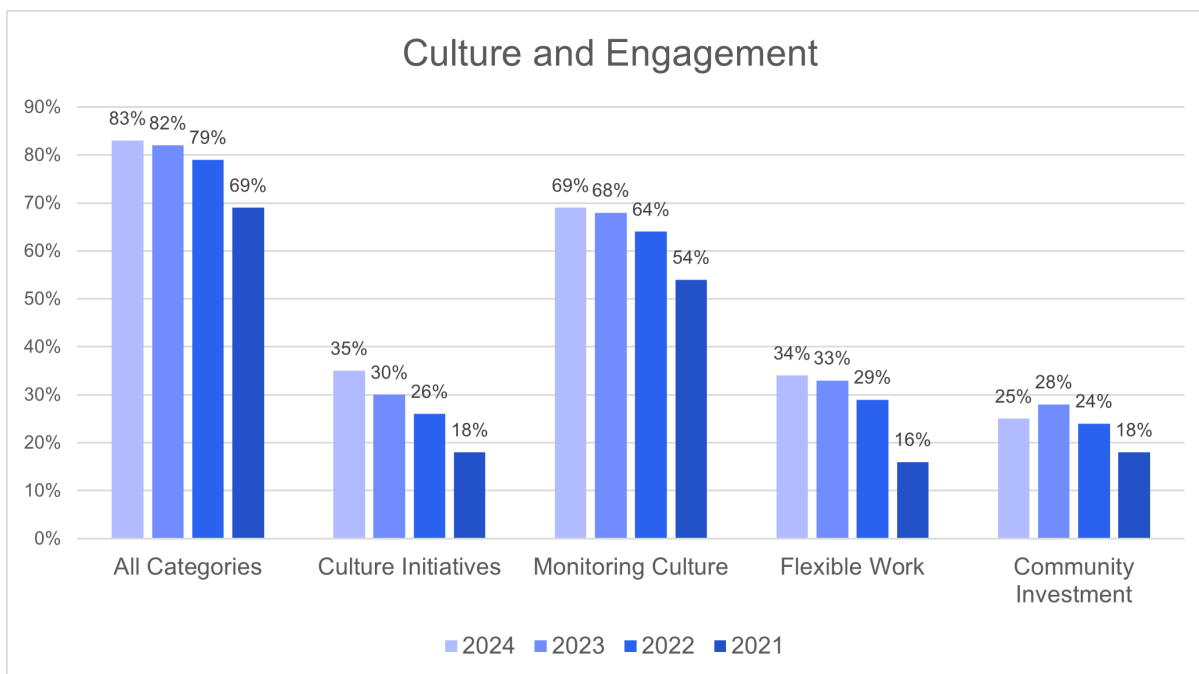


F. Culture and Engagement

In addition to the many instances where companies included general descriptions of their commitment to company culture and values, 83% of S&P 100 companies discussed specific initiatives they were taking related to culture and engagement in one or more of the following categories:

- Culture and engagement initiatives.** Specific disclosures relating to practices and initiatives undertaken to build and maintain their culture and values have increased steadily each year, with 35% of the companies surveyed providing such disclosure, up from 18% in 2021. These companies most commonly discussed efforts to communicate with employees (e.g., through town halls, CEO outreach, trainings, or conferences and presentations) and to recognize employee contributions (e.g., awards programs and individualized feedback). Many companies also discussed culture in the context of diversity-related initiatives designed to help foster an inclusive culture.
- Monitoring culture.** Of the companies surveyed 69% provided disclosures about the ways that companies monitor culture and employee engagement, up from 54% in 2021. Companies generally disclosed the frequency of employee surveys used to track employee engagement and satisfaction, with some reporting on the results of these surveys, sometimes measured against prior year results or industry benchmarks, and ways in which company management or the board utilized survey results.
- Flexible Work Opportunities.** About one-third of S&P 100 companies describe flexible working arrangements, including remote or hybrid work or scheduling adjustments to accommodate different ways of working, with 34% of companies provided such disclosure in 2024, compared to 16% in 2021. Although many of these companies discussed this topic in previous years, past mentions of measures related to flexible work environments were generally in connection with COVID-related safety concerns, whereas recent discussions are increasingly related to talent acquisition and retention.

- Community investment.** Some companies disclosed information about community investment, partnerships, donations, or volunteer programs sponsored by the company, with 25% of companies surveyed providing such disclosure in 2024, compared to 28% in 2023 and 18% in 2021. Many companies discussed their community investment efforts as offshoots of or in conjunction with their diversity, equity, and inclusion efforts.



G. COVID-19

The number of S&P 100 companies that included information regarding COVID-19 and its impact on company policies and procedures or on employees dropped to only one companies making such disclosure, compared to 34% in 2023 and 70% in 2022. This sharp decline in COVID-19 disclosures is consistent with a more general trend of companies discussing COVID-19 less frequently as a result of its decreasing significance and illustrates the expected evolution of disclosure resulting from a principles-based framework.

H. Human Capital Management Governance and Organizational Practices

Just over half of S&P 100 companies (54% of those surveyed, compared to 40% in 2021) addressed their governance and organizational practices (such as oversight by the board of directors or a committee and the organization of the human resources function).

III. Industry Trends

One of the main rationales underlying the adoption of principles-based—rather than prescriptive—requirements for human capital disclosures is that the relative significance of various human capital measures and objectives varies by industry. This is reflected in the following industry trends that we observed:[\[7\]](#)

- **Technology Industries** (*E-Commerce, Internet Media & Services, Hardware, Software & IT Services, and Semiconductors*). For the 22 companies in the Technology Industries, at least 63% discussed each of talent development and training opportunities, talent attraction, recruitment and retention, employee compensation, employee mental health, and diversity. Compared to the S&P 100 as a whole, relatively uncommon disclosures among this group included part-time and full-time employee statistics (5%), succession planning (9%), supplier diversity (5%), diversity in retention and development (41%), quantitative diversity statistics regarding race/ethnicity and gender (41% and 45%, respectively), and unionized employee relations (18%). However, these industries continued to see increased rates of disclosure compared to the S&P 100 for quantitative turnover rates (41%), flexible work opportunities (45%), culture initiatives (45%), and qualitative pay equity (59%).
- **Finance Industries** (*Asset Management & Custody Activities, Consumer Finance, Commercial Banks, and Investment Banking & Brokerage*). For the 13 companies in the Finance Industries, a large majority continued to include quantitative diversity statistics regarding race (85%) and gender (92%) (matching that of the last two years) and qualitative disclosures regarding employee compensation (92%), and, compared to other industries, a relatively higher number discussed diversity in hiring (85%), employee mental health (77%), flexible work opportunities (69%), pay equity (69%), and quantified their pay gap (46%). Relatively uncommon disclosures among this group included part-time and full-time employee statistics, unionized employee relations, quantitative workforce turnover rates, diversity targets and goals, quantitative new hire diversity, supplier diversity, and workplace safety (in each case less than 16%).
- **Pharmaceutical Industries** (*Biotechnology & Pharmaceuticals*). For the eight companies in the Pharmaceutical Industries, at least 87% discussed each of diversity, workplace safety, monitoring culture, talent attraction and retention, talent development, and employee compensation. Compared to the S&P 100 as a whole, relatively uncommon disclosures among this group included succession planning (13%), quantitative pay gap (0%), and diversity targets and goals (0%). However, these industries continued to see increased rates of disclosure compared to the S&P 100 for supplier diversity (38%), workplace safety (88%), culture initiatives (50%), and flexible work opportunities (75%).

IV. Disclosure Format

The format of human capital disclosures in S&P 100 companies' annual reports on Form 10-K continued to vary greatly.

Word Count. The length of the disclosures ranged from 106 to 1,809 words, with the following statistical trends in the past four years:

	2024	2023	2022	2021
Minimum word count	106	106	109	105

Maximum word count	1,809	2,094	1,995	1,931
Median	913	1,035	959	818
Mean	946	1,002	976	825

Metrics. The disclosure requirement specifically asks for a description of “any human capital *measures* or objectives that the registrant focuses on in managing the business” (emphasis added). Our survey revealed that companies are increasingly providing quantitative metrics, with 84% of companies providing disclosure in at least one of the quantitative categories we discuss above (compared to 87% in 2023, 80% in 2022, and 67% in 2021) and only 8% electing not to include any type of quantitative metrics beyond headcount numbers (compared to 7% in 2023, 10% in 2022 and 14% in 2021).

Graphics. Although the minority practice, 26% of companies surveyed also included tables, charts, graphics or similar formatting used to draw attention to particular elements, compared to 26% in 2023, 24% in 2022 21% in 2021, which were generally used to present statistical data, such as diversity statistics or breakdowns of the number of employees by geographic location.

Categories. Most companies organized their disclosures by categories similar to those discussed above and included headings to define the types of disclosures presented.

V. Upcoming Rulemaking and Investor Advisory Committee Recommendations

At its meeting on September 21, 2023, the Commission’s Investor Advisory Committee (“IAC”) approved subcommittee recommendations (the “IAC Recommendations”) to expand required human capital management disclosures.^[8] The IAC Recommendations contain prescriptive disclosure requirements—many of which have been previously considered as part of the 2020 rulemaking—for various quantitative metrics in the business description of Form 10-K under Item 101(c) of Regulation S-K (including headcount, turnover, compensation, and demographic data) as well as narrative disclosure in Management Discussion and Analysis. For details regarding the IAC Recommendations, please refer to “*Form 10-K Human Capital Disclosures Continue to Evolve*,” available [here](#).

According to the most recent Regulatory Flexibility agenda, a human capital management rule proposal that was originally slated for October 2021 was expected to be issued in October 2024.^[9] However, no rule was ever proposed, and many expect regulatory priorities to change with the upcoming shift in the administration, including SEC Chair Gary Gensler’s upcoming departure on January 20, 2025. We therefore do not expect that the Commission will be adopting IAC’s recommendations in the near term as Republican commissions have in the past generally favored principles-based disclosure over prescriptive disclosure requirements.

VI. Comment Letter Correspondence

Comment letter correspondence from the staff of the Division of Corporation Finance (the “Staff”), which often helps put a finer point on principles-based disclosure requirements like this one, has

shed relatively little light on how the Staff believes the new requirements should be interpreted. Consistent with what we found at this time in the prior three years, the comment letters, all of which involved reviews of registration statements, were generally issued to companies whose disclosures about employees were limited to the bare-bones items companies have discussed historically, such as the number of persons employed and the quality of employee relations. From these companies, the Staff simply sought a more detailed discussion of the company's human capital resources, including any human capital measures or objectives upon which the company focuses in managing its business. There were also a few comment letters where the Staff asked companies to clarify statements in their human capital disclosures or expand their human capital disclosures based on related risks identified in their risk factors.^[10] Based on our review of the responses to those comment letters, we have not seen a company take the position that a discussion of human capital resources was immaterial and therefore unnecessary.

VIII. Conclusion

Based on our survey, companies continue to be thoughtful about their human capital disclosures—expanding their disclosures in some areas (e.g., culture initiatives and pay equity) and reducing them in others (e.g., COVID-19, diversity targets and goals, diversity in promotion, and community investment)—in response to ever-changing circumstances. That is precisely what principles-based disclosure rules are designed to elicit.

To that end, as companies prepare for the upcoming Form 10-K reporting season, they should consider the following:

- Confirm (or reconfirm) that the company's disclosure controls and procedures support the statements made in human capital disclosures knowing that controls in the HR department may not be as rigorous as accounting controls. These disclosures create legal liability risks and should be treated accordingly.
- Companies may want to compare their own disclosures against what their industry peers did these past four years, including specifically any notable changes to disclosures made in the past year.
- Remind stakeholders internally that these disclosures likely will continue to evolve. This is especially true with the change in administration that could result in companies focusing on fewer or different issues. The types of measures and objectives that a company focuses on in managing its business and that are material to each company may also change in response to current events, as was shown by essentially the complete removal of COVID-19 related disclosures from 10-K filings the past two years and the decrease in disclosures relating to diversity targets and goals over the same period.
- If you continue to disclose targets, expect the SEC staff to ask you to disclose the progress that management has made. You may wish to reconsider the utility in disclosing specific targets.
- Addressing in the upcoming disclosure, if not already disclosed, the progress that management has made with respect to any significant objectives it has set regarding its

human capital resources as investors are likely to focus on year-over-year changes and the company's performance versus stated goals.

- Addressing significant areas of focus highlighted in engagement meetings with investors and other stakeholders. In a 2024 survey, human capital management was one of the top five issues (aside from financial performance) most important to investors when evaluating companies.[\[11\]](#)
- Revalidating the methodology for calculating quantitative metrics and assessing consistency with the prior year. Former Chairman Clayton commented that he would expect companies to “maintain metric definitions constant from period to period or to disclose prominently any changes to the metrics.”

The following Gibson Dunn attorneys assisted in preparing this update: Brian Lane, Julia Lapitskaya, Ronald Mueller, Michael Titera, and Meghan Sherley.

Gibson Dunn's lawyers are available to assist with any questions you may have regarding these developments. To learn more about these issues, please contact the Gibson Dunn lawyer with whom you usually work in the firm's [Securities Regulation and Corporate Governance](#) or [Labor and Employment](#) practice groups, or any of the following practice leaders and members:

Securities Regulation and Corporate Governance:

[Elizabeth Ising](#) – Co-Chair, Washington, D.C. (+1 202.955.8287, eising@gibsondunn.com)
[James J. Moloney](#) – Co-Chair, Orange County (+1 949.451.4343, jmoloney@gibsondunn.com)
[Lori Zyskowski](#) – Co-Chair, New York (+1 212.351.2309, lzyskowski@gibsondunn.com)
[Aaron Briggs](#) – San Francisco (+1 415.393.8297, abriggs@gibsondunn.com)
[Thomas J. Kim](#) – Washington, D.C. (+1 202.887.3550, tkim@gibsondunn.com)
[Brian J. Lane](#) – Washington, D.C. (+1 202.887.3646, blane@gibsondunn.com)
[Julia Lapitskaya](#) – New York (+1 212.351.2354, jlapitskaya@gibsondunn.com)
[Ronald O. Mueller](#) – Washington, D.C. (+1 202.955.8671, rmueller@gibsondunn.com)
[Michael Scanlon](#) – Washington, D.C. (+1 202.887.3668, mscanlon@gibsondunn.com)
[Michael A. Titera](#) – Orange County (+1 949.451.4365, mtitera@gibsondunn.com)

Labor and Employment:

[Jason C. Schwartz](#) – Co-Chair, Washington, D.C. (+1 202.955.8242, jschwartz@gibsondunn.com)
[Katherine V.A. Smith](#) – Co-Chair, Los Angeles (+1 213.229.7107, ksmith@gibsondunn.com)

on any specific facts or circumstances. Gibson Dunn (and its affiliates, attorneys, and employees) shall not have any liability in connection with any use of these materials. The sharing of these materials does not establish an attorney-client relationship with the recipient and should not be relied upon as an alternative for advice from qualified counsel. Please note that facts and circumstances may vary, and prior results do not guarantee a similar outcome.

If you would prefer NOT to receive future emailings such as this from the firm,
please reply to this email with "Unsubscribe" in the subject line.

If you would prefer to be removed from ALL of our email lists,
please reply to this email with "Unsubscribe All" in the subject line. Thank you.

© 2024 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit our [website](#).



IPO and Public Company Readiness: Advance Planning for 2025 and 2026 IPOs

Corporate Governance and ESG Considerations

November 12, 2024

GIBSON DUNN

Today's Speakers



Aaron Briggs

Partner | Securities Regulation and
Corporate Governance

San Francisco



Hillary H. Holmes

Partner | Capital Markets (Co-Chair)

Houston



Lori Zyskowski

Partner | Securities Regulation and
Corporate Governance (Co-Chair)

New York

MCLE Information

The information in this presentation has been prepared for general informational purposes only. It is not provided in the course of an attorney-client relationship and is not intended to create, and receipt does not constitute, an attorney-client relationship or legal advice or to substitute for obtaining legal advice from an attorney licensed in the appropriate jurisdiction.

- This presentation has been approved for **1.0 General credit**
- Participants must submit the form by **Tuesday, November 19th** in order to receive CLE credit

CLE Form Link: https://gibsondunn.qualtrics.com/jfe/form/SV_77GVOhWgo6Y8MB0

Most participants should anticipate receiving their certificate of attendance in 4-6 weeks following the webcast

All questions regarding MCLE Information should be directed to CLE@gibsondunn.com

About this Webcast Series

IPO & Public Company Readiness: Advance Planning for 2025 & 2026

- This webcast: provides an overview of the key corporate governance decisions a company will need to make as it prepares for an IPO

- Previous webcast:

Executive Compensation & Employee Benefits (linked [here](#)) October 2024

- Upcoming webcasts:

Regulatory Compliance January 2025

Cybersecurity & Data Privacy January 2025

Private Equity Sponsor-Backed Portfolio Companies February 2025

Structuring & Tax Issues March 2025

Risk Management & Financial Systems April 2025

International Perspectives May 2025



Agenda

01 Introduction

02 Board Composition

03 Board Structure

04 Governance Structure

05 Corporate Compliance Policies

06 Other Considerations

07 So Now What?

Introduction

01

Overview of Governance Decision-Making

Basic Principle

A company generally has wide latitude to determine the appropriate board and governance structure to support execution of long-term strategy, particularly at IPO

Selected Considerations for Making Governance Decisions

- Flexibility: preserve board's ability to act in shareholders' best interests based on facts & circumstances
- Shareholder base: decision-making may differ depending on whether the company is controlled or otherwise has a significant shareholder, founder, etc.
- Activist defense: protect company from inappropriate threats for corporate control, particularly in the early stages of the company's life cycle
- Market practice: maintain alignment with peers or have good reason not to
- State law: shareholder rights, director responsibilities & board operations
- Stock exchange / SEC rules: director independence, committee composition & responsibilities, code of conduct and various disclosure requirements
- Investor / proxy advisor expectations: view anti-takeover protections as inhibiting shareholder rights; may vote against board or specific committee members at shareholder meetings based on certain IPO-related governance decisions
- Latest trends: consider board diversity as well as ESG strategies, cybersecurity, risk management & potential disclosures

Task List

Key Governance Action Items to Get Ready for the IPO

- ✓ Assemble public company board
- ✓ Decide on important structural points
- ✓ Draft key documents
- ✓ Identify executive officers
- ✓ Protect directors & officers
- ✓ Build out key public company functions
- ✓ Establish & augment controls
- ✓ Consider other regulations & stakeholder preferences
- ✓ Don't forget about other tasks

Board Composition

02

Board Composition Overview



Regulatory Independence

What?

- Basic idea: independent directors do not have any relationship with the company that would interfere with their ability to exercise independent judgment in carrying out their duties
- Key NYSE/Nasdaq tests to assess: (not exclusive, 3-yr lookback, look at both directors & family members)
 1. No employment with company
 2. No compensation from company >\$120k besides director fees
 3. No business relationship with company above materiality thresholds (NYSE: \$1m/2% rev | Nasdaq: \$200k/5% rev)
 4. No comp committee interlocks
 5. No employment with outside auditor
- Audit & Comp Committee members: subject to heightened independence standards (see next slide)

GIBSON DUNN

Why?

- Good governance: key role of board is to oversee management performance
- NYSE/Nasdaq requirements: (controlled companies generally exempt)
 - Majority independent board
 - Fully independent committees (audit, compensation, nominating)

Phase In	Requirement
At IPO	1+ independent director on each committee
90 days later	Majority+ independent committees
1 year later	Fully independent committees + majority independent board

- Certain investor expectations:
 - May expect substantially independent boards (e.g., 2/3)
 - In some cases have their own, more stringent definitions

How?

- Directors complete D&O questionnaires, including questions designed to assess independence
- Legal vets responses and conducts additional diligence if necessary
- Finance runs directors and their family members and affiliated entities through AR/AP systems to confirm no payments
- Board ultimately makes the determination as to each director's independence, considering all relevant facts and circumstances

Public Disclosure

Identifies who's independent + relationships considered by the board

Heightened Independence Standards for Committee Members

Independence Factor	Audit Committee	Compensation Committee
Receive other comp from company besides director fees	Prohibited	Board must take into account in assessing independence
Qualify as an affiliate of company (or affiliate of a large shareholder)	Prohibited	Board must take into account in assessing independence
Helped prepare company financials in past 3 years	Prohibited	N/A
Have a material interest in a related party transaction	N/A	Generally prohibited unless special procedures adopted to approve equity

Financial Expertise

What?

- Basic idea: all audit committee members are expected to be financially literate (i.e., can read & understand a balance sheet, income statement & cash flow statement), and one is expected to be a financial expert
- SEC requirements to be an expert:
 1. Understanding of GAAP & financials
 2. Ability to assess application of GAAP for estimates/accruals/reserves
 3. Experience preparing, auditing, analyzing & evaluating (or supervising) financials of same breadth/complexity as company's
 4. Understanding of internal control over financial reporting
 5. Understanding of audit committee functions

Why?

- Good governance: role of audit committee is to oversee preparation & integrity of the company's financials
- SEC requirements:
 - Must have at least one audit committee financial expert (or explain why not)
 - Must identify the expert & disclose whether they are independent and describe their experience if they qualify outside of traditional means
 - No impact on director duties/liability
- NYSE/Nasdaq requirements:
 - All audit committee members must be financially literate
 - One audit committee member must be a financial expert (SEC financial expert satisfies the requirement)

How?

- Directors complete D&O questionnaires, including questions designed to assess financial expertise
- Legal vets responses and conducts additional diligence if necessary
- Board ultimately makes the determination as to who qualifies

Ways to Qualify as an Expert

- Education & experience as CFO, CAO, Controller or Auditor
- Experience actively supervising one of the above (possibly CEO)
- Experience overseeing or assessing company performance with respect to preparation, auditing or evaluation of financials
- OR other relevant experience

Diversity

What?

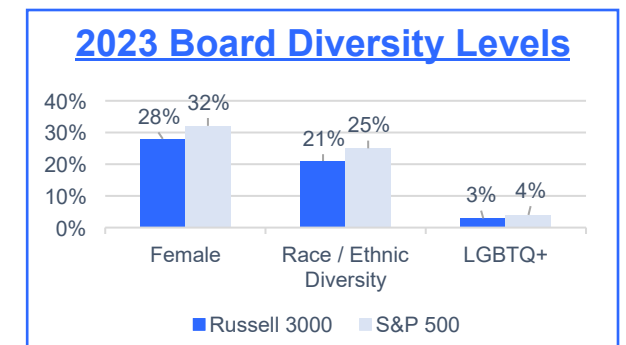
- Basic idea: boards generally should be diverse across a range of characteristics, backgrounds & perspectives
- No single definition, but key traits often looked at by boards include:
 1. Gender
 2. Race/ethnicity
 3. Nationality
 4. Cultural background
 5. Sexual orientation
 6. Age
 7. Veteran status
 8. Disability
 9. Education

Why?

- SEC requirements: must disclose policy on diversity, how the board assesses its effectiveness and whether diversity was considered in the selection of a director
- Nasdaq requirements: (no equivalent NYSE requirements)
 - Board composition: must have at least 1 female director & 1 director who is an underrepresented minority or LGBTQ+ or explain why not (subject to exceptions for smaller boards or companies)
- Disclosure: matrix showing board-level data on gender diversity and race/ethnicity/LGBTQ+ diversity
- Investor expectations: often have specific numerical expectations on board diversity (see next slide)

How?

- Directors complete D&O questionnaires, including voluntary questions for director to self-ID across various characteristics and indicate whether they consent to disclosure
- Board
 - Establishes policy on diversity & criteria for specific director searches
 - Sometimes adopts a “Rooney Rule” policy (i.e., commitment to include diverse candidates in the pool from which directors are selected)



Source: Conference Board, *How Board Diversity Can Contribute to Board Effectiveness* (Nov. 2023)

Current Policies on Board Diversity

(as of October 2024)

Institution*	Gender	Race/Ethnicity
<i>Proxy Advisory Firms</i>		
ISS	1+	1+ (S&P 1500/Russell 3k)
Glass Lewis	30%+	1+
<i>Selected Institutional Investors</i>		
BlackRock	2+ (plus 30% diverse overall)	1+ (plus 30% diverse overall)
Vanguard	Facts & circumstances based on sufficiency of progress	Facts & circumstances based on sufficiency of progress
Fidelity	2+ (10+ member boards)	1+
State Street	30%+ (Russell 3k)	1+ (S&P 500/FTSE 100)
JPMorgan	1+	1+

Investors may vote against the election of the nominating committee when these policies are not satisfied

**Policies for 2025 proxy season are not yet available*

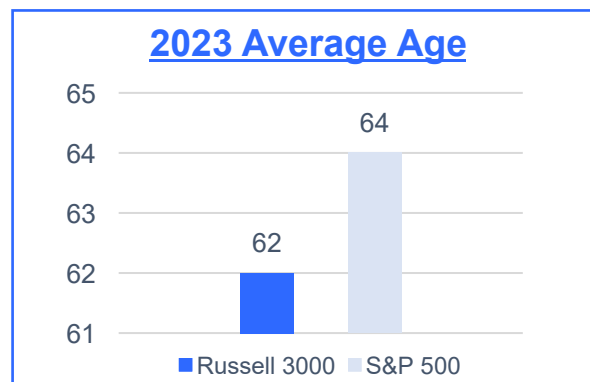
Other Characteristics

Skills and Experiences

- Basic idea: board should have a mix of skills and experiences to support board's role in overseeing strategy and major risks facing the company
- SEC requirements: for each director, must disclose experience, qualifications and skills that led to board's determination they should serve on the board, in light of the company's business and structure
- Commonly sought experiences:
 1. CEO / Leadership
 2. Industry / Operations / Global
 3. Regulatory / Government / Legal
 4. Technology / IT / Cyber
 5. Finance / Accounting / Investment
 6. Risk Management

Age

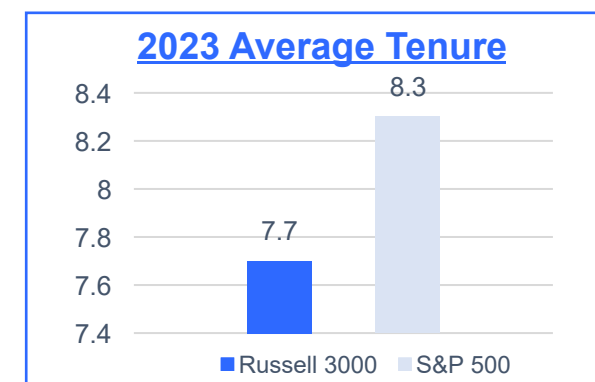
- Basic idea: directors should collectively represent a mix of ages, and boards may consider whether to institute a director retirement policy (e.g., must retire at age 72 or 75)
- SEC requirements: must disclose age of each director
- Investor expectations: not a significant focus area
- Market data:



Source: Conference Board, *Taking a Long-Term Approach to Board Composition* (Sept. 2023)

Board Tenure

- Basic idea: directors should collectively represent a mix of tenures; some boards have term limits, but those are not common
- SEC requirements: must disclose how long each director has served
- Investor expectations: generally look for a mix of tenures & refreshment; some assess average tenures
- Market data:



Source: Conference Board, *Recent Trends in Board Composition and Refreshment in the Russell 3000 and S&P 500* (Dec. 2023)

Overboarding

What?

- Basic idea: there often is an expectation – whether general or specific – that directors will limit (to varying degrees depending on the director’s other commitments) the number of public company boards on which they serve
- Heightened scrutiny and/or stricter expectations often applied to directors in the following categories:
 1. CEOs of a public company
 2. Officers of a public company
 3. Board Chairs or Lead Independent Directors
 4. Audit Committee members

Why?

- Good governance: directors should have sufficient capacity to devote to company matters, and this has become even more critical as board oversight obligations have continued to increase (e.g., risk, cyber, ESG)
- SEC requirements: must disclose for each director all pubco boards on which they serve, as well as identify any director who attended <75% of board/committee meetings
- NYSE requirements: audit committee members limited to 3 pubco audit committees absent a board determination + additional disclosure (no equivalent Nasdaq requirements)
- Investor expectations: often have specific numerical expectations on when they consider a director to be overboarded (see next slide)

How?

- Directors complete D&O questionnaires, including questions designed to assess current obligations and compliance with any company policies
- Board
 - Establishes a policy on overboarding (ranging from a general statement to specific numerical limits)
 - May require nominating committee approval (or at least notice) before directors can join additional boards
 - Monitors compliance in connection with annual nomination process

Current Policies Around Overboarding

(as of October 2024)

Institution*	PubCo CEO / Officer (max # of pubco boards)	Other Directors[†] (max # of pubco boards)
<i>Proxy Advisory Firms</i>		
ISS	3 (2 + own board)	5
Glass Lewis	2 (1 + own board)	5
<i>Selected Institutional Investors</i>		
BlackRock	2 (1+ own board)	4
Vanguard	2 (1+ own board)	4
Fidelity	2	5
State Street	2	4
JPMorgan	3 (2 + own board)	4

Investors may vote against the election of any director who does not satisfy these policies

**Policies for 2025 proxy season are not yet available*

†Does not include separate policies for board leadership positions

Managing Conflicts and Antitrust Issues

Conflicts of Interest

- Basic idea: boards must manage conflicts of interest that could impair a director's ability to make decisions that are in the best interests of shareholders
- NYSE/Nasdaq requirements: companies must have codes of conduct addressing actual and apparent conflicts, and any waivers granted to directors must be disclosed within 4 business days
- Examples of conflict situations:
 - Director or family member does business with a competitor
 - Company does business with a director's or family member's business
 - Director stands on both sides of a company transaction

Antitrust Issues

- Basic idea: antitrust laws prohibit interlocking director & officer roles that could be anti-competitive
 - Clayton Act: directors are prohibited from serving as a director or officer of a competitor of the company (subject to de minimis thresholds)
 - Sherman Act: certain director affiliations with a competitor or supplier of the company may require firewall procedures
- Process for managing:
 - D&O questionnaire process
 - Notification/approval requirements to nominating committee
 - Director training
 - Potential director recusal

Board Structure

03

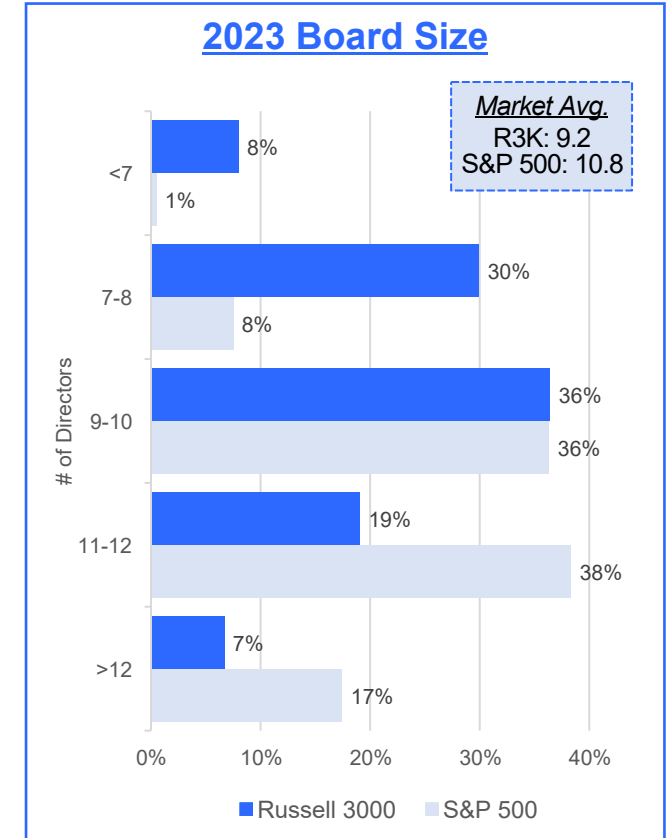
Board Size

Basic Principles

- No legal or regulatory requirements around board size
- Boards have flexibility to determine appropriate size for the company
- Generally not a significant issue for the investment community, but Glass Lewis generally says optimal board size is 5 to 20

Finding the Sweet Spot

- Need enough directors to support the board's oversight of strategy and risk management as well as to staff the key committees
- But, avoid having too many directors, which can lead to complexity and inefficient decision-making and board processes



Source: Conference Board, *Taking a Long-Term Approach to Board Composition* (Sept. 2023)

Board Leadership Structure

3 Options

1. Combined Chair & CEO

- What this is: same person serves as both chair and CEO
- Positives: CEO viewed as well-positioned to focus board on key issues, promotes more efficient governance processes
- Negatives: CEO distraction, conflicts due to lack of independent oversight by chair, some investor pushback

2. Separate Executive Chair

- What this is: separate person who is not independent (e.g., Founder, former CEO) serves as chair
- Positives: allows CEO to focus on the business, provides some independent oversight
- Negatives: less efficient governance processes due to duplication & blurred lines of responsibility

3. Separate Independent Chair

- What this is: separate person who is independent serves as chair
- Positives: allows CEO to focus on the business, provides greatest independent oversight
- Negatives: less efficient governance processes due to duplication & blurred lines of responsibility

Lead Independent Director

- Basic idea: if chair is not independent (options 1 or 2), investment community expects LID appointment for independent board oversight
- ISS has specific expectations around LID responsibilities:
 - Preside at board meetings when chair isn't present
 - Preside at executive sessions of independent directors
 - Call meetings of independent directors
 - Review/approve information sent to board
 - Review/approve board meeting schedules/agendas
 - Available to meet with major investors upon request

Board Committee Structure

3 Key Committees + Any Other Committees Helpful for Board Oversight

	Audit*	Compensation*	Nominating*
Committee Size	Required to have at least 3	Required to have at least 2	No specific requirements
Meeting Frequency	4x+/year	Depends on company	Depends on company
Key Third Parties	Independent auditor	Independent comp consultant	Director search firm
Traditional Oversight Areas	<ul style="list-style-type: none"> Accounting & financial reporting processes Internal controls & disclosure controls Compliance & conflicts of interest Performance of outside auditors Risk oversight processes 	<ul style="list-style-type: none"> Compensation philosophy & programs CEO goal-setting, evaluation & comp Executive officer evaluation & comp Equity plan admin/grants Incentive & director comp Executive succession planning 	<ul style="list-style-type: none"> Board composition & structure Director succession planning/recruitment Committee composition & leadership structure Corporate governance practices Board operations, including evaluations
Newer Focus Areas	<ul style="list-style-type: none"> Cybersecurity 	<ul style="list-style-type: none"> Human capital management 	<ul style="list-style-type: none"> Sustainability & ESG

*Committee charter publicly disclosed

Examples of potential additional committees
 EHS, Executive, Finance, Public Policy, M&A, Risk, Sustainability, Technology

Key Board Oversight Processes

Critical to Establish Appropriate Operating Rhythms

Board Oversight of Strategy / Execution

- Basic idea: to fulfill their fiduciary duties, boards should establish robust processes to oversee company strategy and monitor execution to help maximize shareholder value
- Strategy: typically done in a separate, dedicated board meeting (sometimes off-site) to focus on long-term strategy development
- Execution: typically monitored at every regular board meeting through updates from the CEO and other members of management, but updates in between meetings may be appropriate as well

Board Oversight of Risk

- Basic idea: to fulfill their fiduciary duties, boards should establish robust processes to oversee the most significant risks facing the company, including implementing an appropriate reporting system
- Why this is important: although there is generally a high bar under DE law for directors to be liable for failures of risk oversight, recent cases show it's not an impossible standard to satisfy
- What this entails:
 - Clear roles & responsibilities: who on the board (full board vs. committee) and in management is responsible for each risk?
 - Robust reporting system: what's the appropriate frequency and substance of the reporting?
 - Alignment with ERM framework: does the reporting system capture all of the key risks facing the company? Is there a built-in mechanism to revisit this periodically?
 - Engaged directors: are directors sufficiently engaged, asking questions & monitoring follow-ups?
 - Appropriate delegations of authority: what can management approve without going to board?

Governance Structure

04

Positioning the Company Generally

- Wide latitude pre-IPO to adopt the post-IPO certificate of incorporation and bylaws
- No single governance structure appropriate for all IPO co's, and will depend on factors like size, industry, investor base, desired positioning on governance issues
- Common for IPO co's to start with a more protective governance structure (much more difficult to add later on), which then evolves and becomes less protective over time in response to investor engagement

Key Factors Impacting Rate of Change

- **Company growth:** as market cap grows, company will increasingly be a target for shareholder proposals and other investor campaigns – for example, of the total # of proposals submitted to companies each year, roughly:

~5%

Small-caps

~10%

Mid-caps

~85%

Large-caps

- **Evolving shareholder base:** as large asset managers take bigger positions and the base shifts away from venture/hedge/PE funds, proxy advisor (ISS/Glass Lewis) influence is likely to grow
- **Voting/reputational concerns:** certain practices may generate criticism from investors and negative votes for directors; level of responsiveness/proactivity will depend on philosophical approach
- **Changing peer practices:** while company's existing practices at IPO may be in line with market, as company grows, at some point that may no longer be the case

Director Elections / Vacancies

Decision Point	Basic Idea	Activism Considerations	Investment Community View	Typical Approach for IPO Companies
Classified vs. Declassified Board	<p><u>Classified</u>: directors are placed into 3 different classes, with only 1 class elected at each annual meeting (3-yr terms)</p> <p><u>Declassified</u>: all directors elected annually (1-yr terms)</p>	Classified board viewed as providing strong anti-takeover protection since potential acquirer can't replace a majority of the board at once (plus under DE law classified directors can be removed only for cause)	Classified boards generally are disfavored; often a standalone basis for votes against directors <i>~85% support for shareholder proposals</i>	Classified board, coupled with director removal only for cause per state law (but different considerations for controlled companies) <u>Hybrid approach</u> : include with built-in sunset
Plurality vs. Majority Vote to Elect Directors	<p><u>Plurality</u>: means those with the most votes elected</p> <p><u>Majority</u>: directors must receive more votes "for" than "against"</p>	Plurality is an easier standard to get directors elected, but this generally isn't a concern in a proxy contest (plurality applies no matter what)	Plurality voting outside a proxy contest generally is disfavored <i>~50% support for shareholder proposals</i>	Plurality vote standard <u>Hybrid approach</u> : include coupled with director resignation policy if fail to get majority vote
Vacancies Filled Only by the Board	Provides that any vacancies on the board can be filled only by the board (not by shareholders)	Prevents an activist from taking action to increase the size of the board and then filling the resulting vacancy	Does not receive significant focus	Vacancies filled only by board

Shareholder Action / Voting

Decision Point	Basic Idea	Activism Considerations	Investment Community View	Typical Approach for IPO Companies
Shareholders Act by Written Consent	Allows shareholders to act by written consent between shareholder meetings	May facilitate activism in between annual meetings, particularly without appropriate guardrails	Generally favor a shareholder right to act by written consent <i>~40% support for shareholder proposals</i>	Prohibit (but different considerations for controlled companies)
Shareholders Call Special Meetings	Allows shareholders to call special meetings in between annual meetings; may facilitate takeovers	May facilitate activism in between annual meetings, particularly without appropriate guardrails	Generally favor a shareholder right to call special meetings <i>~50% support for shareholder proposals</i>	Prohibit (but different considerations for controlled companies)
Supermajority Voting Provisions	Greater-than-majority vote required to remove directors and/or amend bylaws & certain charter provisions	Makes it more difficult for an activist to change the board or governance documents	Generally disfavored; often a standalone basis for votes against directors <i>~65% support for shareholder proposals</i>	Include, often at 66% (but different considerations for controlled companies) <u>Hybrid approach</u> : include with built-in sunset
Dual-class Common Stock	Can be used to provide lower voting rights for different share classes (high-vote / low- or no-vote stock)	Concentrates voting power in the founders/management team post-IPO	Generally disfavored; often a standalone basis for votes against directors <i>~30% support for shareholder proposals</i>	Not typical, but more common in founder-led co's <u>Hybrid approach</u> : include with built-in sunset

Other Key Governance Structure Items in Formation Documents

Certificate of Incorporation*

- Blank-check preferred stock: allows board to issue preferred stock and set rights without shareholder approval, which can facilitate adoption of a shareholder rights plan down the road
- Exclusive forum: designates specific court(s) as exclusive venue(s) for certain shareholder lawsuits, both at the state level (internal corporate claims) and federal level (Securities Act claims)
- Exculpation of directors and officers: eliminates monetary damages for breach of fiduciary duty of care (subject to certain exceptions); DE law recently amended to permit this for officers
- Statutory freeze for “interested shareholder” transactions: default provision in DE that, subject to certain exceptions, restricts tender offers by 15%+ shareholders for 3 years, unless company opts out in the charter (not typical to opt out)

Bylaws*

- Advance notice of shareholder business: sets forth timing, informational and other procedural requirements for shareholders that want to nominate directors or submit other business to be considered at the annual shareholder meeting
- Proxy access: permits shareholders that meet certain ownership and holding requirements to nominate directors and have them included in the company’s proxy materials (not typical to include for IPO companies)

Choosing Legal & Regulatory Regimes

State of Incorporation

Key Considerations

- Legal system: varies in terms of depth and breadth of established case law precedents, experience and specialization of the courts in handling corporate disputes
- Fiduciary duties: varies in terms of whether focused on maximizing shareholder value vs. permitting broader stakeholder focus
- Standard for court review of board decisions: varies in terms of level of deference to the board's business judgment vs. application of enhanced scrutiny or entire fairness standards
- Exculpation of directors from liability: varies in terms of scope of elimination of liability for directors, including whether it is limited to duty of care or also applies to duty of loyalty
- Books and records inspection rights: permit shareholders to inspect the company's books and records, which can be a precursor to litigation
- Fees and taxes: annual franchise fees and taxes owed in different jurisdictions at different rates

Choosing Legal & Regulatory Regimes

Stock Exchange Listing:

NYSE vs. Nasdaq

Key Considerations

- Quantitative initial and continued listing standards: e.g., minimum requirements for number of holders, shares outstanding, trading price, market value of publicly held shares, income, market cap
- Cost: initial listing fee and annual fee
- Packages offered: market services and IR products
- Corporate governance requirements: similar, but some notable differences...

Requirement	NYSE	Nasdaq
Director independence	<u>Business test</u> : greater of \$1M or 2% of revenues	<u>Business test</u> : greater of \$200k or 5% of revenues
Committee independence	No hardship exemption	Hardship exemption (permit non-independents in limited circumstances)
Nominating committee	Required	Not required (can be done by independent directors)
Internal Audit function	Required	Not required
Governance guidelines	Required	Not required
Board diversity	Not required	Comply or explain
Related party transactions	Stricter on prior approval	Less strict on prior approval
Annual CEO certification	Required	Not required

Corporate Compliance Policies

05

Audit Committee-Related Policies

Auditor Services Approval*

- Legal requirement: all audit and non-audit services performed by independent auditor must be pre-approved by audit committee
- What the policy does: sets forth procedures for handling the pre-approval process, including reporting and documentation requirements
- Key decisions: delegation threshold to the chair to handle approvals in between committee meetings

Auditor Employee Hiring

- Legal requirement: to prevent impairing the independence of the independent auditor, companies are restricted from hiring certain current and former employees of the auditor into certain financial reporting oversight and accounting roles, unless various conditions are satisfied (e.g., no operational influence or financial ties with auditor, cooling-off period)
- What the policy does: sets forth the various hiring conditions and identifies the financial reporting oversight roles at the company

Whistleblower Procedures

- Legal requirement: audit committees must establish procedures for handling complaints regarding controls, accounting and auditing matters, including allowing employees to submit anonymously
- What the policy does: sets forth who handles at management level, when complaints get escalated to committee, and how investigations are handled
- Key decisions: broadening of policy to cover complaints of misconduct generally, criteria for escalating to committee

Compensation Committee-Related Policies

For more info
check out our
[exec comp](#)
[webcast](#)

Compensation Clawback*

- Legal requirement: NYSE and Nasdaq require policy for mandatory no-fault recoupment of incentive comp from officers in the event of a financial statement restatement
- What the policy does: sets forth procedures for assessing whether recoupment is triggered and calculating recoverable amount
- Key decisions: whether to broaden policy to cover additional people, types of compensation, types of triggers (e.g., misconduct)

Equity Grant Timing*

- Legal requirement: companies must disclose practices around timing of granting option awards in relation to the disclosure of MNPI and disclose certain info about NEO option grants made close in time to MNPI release; companies may adopt policy to facilitate this disclosure
- What the policy does: identifies when and under what circumstances equity awards can and cannot be granted
- Key decisions: timing of annual equity grants, how to handle closed trading windows

Stock Ownership Guidelines*

- Legal requirement: not required, but common for companies to adopt to ensure D&Os have “skin in the game” and further align D&O interests with shareholders
- What the guidelines do: set forth the required holdings levels, phase-in schedule and how holdings are calculated
- Key decisions: ownership levels, how far down into the organization to go, treatment of outstanding equity awards, any retention features

Nominating/Governance Committee-Related Policies

Governance Guidelines*

- Legal requirement: NYSE requires corporate governance guidelines
- What the guidelines address: board operations, director qualifications, responsibilities, compensation, performance evaluations, access to management & advisors, orientation & continuing ed, management succession
- Key decisions: overboarding limits, director changes in jobs/boards, diversity policy, age/term limits, categorical independence standards

Code of Conduct*

- Legal requirement: NYSE and Nasdaq require code of conduct for directors/officers/employees
- What the code must address: conflicts of interest, corporate opportunities, confidentiality, fair dealing, proper use of assets, legal/regulatory compliance, reporting of illegal or unethical behavior, code enforcement, accurate & timely SEC reporting, amendments/waivers
- Typical additional topics: gifts, dealing with governmental officials, FCPA compliance, environmental/health/safety

Related Party Transactions*

- Legal requirement: company transactions >\$120k in which 5% holders, directors, officers or family members have a material interest must be approved by a committee and disclosed
- What the policy does: sets forth procedures for escalating to committee and approval criteria
- Key decisions: delegation threshold to the chair to handle approvals between committee meetings; categories of pre-approved transactions; escalation thresholds to committee

Other Key Policies

Insider Trading*

- Legal requirement: employees and directors are prohibited from trading in company securities when they have MNPI, and companies are required to maintain reasonable controls to help prevent
- What the policy does: sets forth procedures for when and how trading can occur (e.g., blackout periods, pre-clearance)
- Key decisions: who is covered, whether other companies' securities are covered, hedging, pledging, 10b5-1 plans

Investor Communications

- Legal requirement: under Reg FD, company officials cannot selectively disclose MNPI to the investment community without disclosing to the market at the same time (e.g., 8-K, PR)
- What the policy does: identifies who is authorized to speak for the company and sets forth procedures for how and when they can speak and policies around dealing with analysts, market rumors and guidance
- Key decisions: designated spokespersons, quiet periods, use of social media

Discl. Committee Charter

- Legal requirement: must have controls designed to ensure info that's required to be disclosed is timely disclosed, and CEO/CFO required to certify quarterly as to effectiveness; as part of this, companies often form a management-level disclosure committee
- What the charter does: sets forth committee membership, responsibilities and operation
- Key decisions: scope of committee's role; membership; delegation/sub-committee procedures

Other Considerations

06

Impact of Recent U.S. Elections on the SEC

- Background: SEC has 5 commissioners who are presidential appointees serving staggered 5-year terms; by design, no more than 3 can belong to same political party
- Current SEC: 3-2 Democratic-led majority under Chair Gensler, with an aggressive enforcement agenda focused on large penalties in several areas as well as a rulemaking agenda largely focused on investor protection/ESG – e.g.:
 - Compensation clawbacks
 - Insider trading / 10b5-1 plans
 - Cybersecurity
 - Climate change
 - Beneficial ownership reporting
- What typically happens upon a change in presidential administration:
 - Resignation of SEC Chair & division directors
 - Designation of Acting Chair from incoming President’s party
 - Appointment (and confirmation by Senate) of new Chair
 - Announcement of new SEC rulemaking & enforcement priorities

Commissioner	Party	Term*
Gary Gensler (Chair)	D	2026
Caroline Crenshaw	D	2024**
Jaime Lizárraga	D	2027
Hester Pierce	R	2025
Mark Uyeda	R	2028

*Can serve up to 18 months beyond term expiration

**Renominated, subject to confirmation

Back to the future with a Clayton-style SEC?

- Greater focus on efficient capital formation?
- Greater focus on reducing regulatory burdens?
- Shift away from ESG rulemaking priorities? E.g., climate change, human capital, board diversity
- Shift in enforcement priorities?
- New views on cryptocurrency?

Evolving Landscape

- Anti-ESG: following years of rapid adoption globally, a growing anti-ESG movement in the US has significantly affected the ESG & DEI landscape
- Broad divergence in approach emerging among U.S. states, such as California & Florida, in the U.S. federal government & globally
 - Europe and UK have continued to advance legislation and other pro-ESG initiatives, including CSRD, that could apply to U.S. companies
 - But in the US, the SEC stayed its long-awaited climate disclosure rules after they were challenged in court, raising uncertainty
- Engagement on ESG continues among some institutional shareholders and other vocal shareholders, including through shareholder proposals (though E&S proposal support is declining)
- Increasing regulation and litigation targeting ESG issues, including greenwashing, as companies release more information & stakeholders scrutinize disclosures
- Board oversight and governance of ESG remains a key consideration across boardrooms, but complicated by evolving ESG & DEI landscape

Regulatory Requirements

SEC Climate Rules

- Background: SEC adopted rules in March 2024, in a 3-2 vote along party lines
- Overview of required climate-related disclosures in Form S-1 registration statement for IPO or annual report on Form 10-K:
 - Governance: board and management governance and practices for climate-related risk identification, assessment, management, and oversight, and related risk processes
 - Risk: climate risks with actual or potentially material impacts on financials, strategy, outlook and business model (but no need to disclose climate expertise on board)
 - GHG emissions: for larger companies, Scope 1 & 2 emissions, if material (but not Scope 3), with independent third-party assurance required on a phased-in basis
 - Targets/goals: climate-related targets or goals established by the company if materially or reasonably likely to materially affect financials, with annual progress updates
 - Transition plans: company-adopted transition plans, scenario analyses, and internal carbon pricing if used to assess material climate risks, plus related material expenditures
 - Financial statement footnote: reporting expenditures and costs of >1% due to “severe weather events,” “other natural conditions,” and certain carbon offsets and RECs
- Legal challenge: rules were challenged and stayed while subject to ongoing multi-district litigation in 8th Circuit

Stay tuned for further developments given change in administration

Regulatory Requirements

Other ESG Rules

California Climate Laws






- Background: in October 2023, California adopted three wide-reaching bills that impose climate reporting requirements for public & private companies doing business or engaging in certain activities in CA
 - GHG emissions reporting: annual disclosure of Scope 1, 2 & 3 emissions + 3rd party assurance (SB 253)
 - Climate risk reporting: biennial disclosure of climate risks and risk management (SB 261)
 - Anti-greenwashing: new disclosures for companies making certain sustainability claims (e.g., net zero, carbon neutral, significant emissions reductions) or deal in voluntary carbon offsets (AB 1305)
- Who's in scope for SB 253/SB 261: among others, companies organized under CA law or meeting sales, property or payroll thresholds in CA, with global annual revenues >\$1B (SB 253) or >\$500M (SB 261)
- Legal Challenge: rules were challenged in the CA Central District, but have not been stayed

EU Laws

- Corporate Sustainability Reporting Directive (CSRD): requires EU & non-EU enterprises with significant EU operations to report material environmental, social and governance matters (using a double materiality framework) in their annual report, including forward-looking, retrospective, qualitative and quantitative information
- Corporate Sustainability Due Diligence Directive (CSDDD): requires EU & non-EU enterprises with significant EU operations to identify and assess adverse human rights and environmental impacts, take steps to prevent/mitigate these impacts, and adopt a Paris Agreement-aligned climate change mitigation transition plan

Stakeholder Expectations

Proxy Advisor & Institutional Investor Policies for 2024

	Climate Change	Human Capital Management	Board Oversight
	<ul style="list-style-type: none"> TCFD-aligned disclosure for significant GHG emitters Disclosure of GHG reduction targets 		<ul style="list-style-type: none"> Disclosure of board oversight of mitigation of climate risks (part of TCFD disclosure)
	<ul style="list-style-type: none"> TCFD-aligned disclosure for S&P 500 in industries w/material GHG risk per SASB Disclosure of GHG reduction targets 	<ul style="list-style-type: none"> Disclosure of human capital risk management and mitigation 	<ul style="list-style-type: none"> Clear disclosure of board-level oversight of E&S issues
	<ul style="list-style-type: none"> ISSB-aligned disclosure Disclosure of Scope 1/2 and material Scope 3 emissions Disclosure of GHG reduction targets (Scope 1/2) & Net Zero-aligned business plan 	<ul style="list-style-type: none"> Disclosure of how approach to HCM is aligned with strategy & biz model Disclosure of steps to advance DEI Disclosure of EEO-1 report 	<ul style="list-style-type: none"> Disclosure of board-level oversight of material risks, including sustainability-related factors
	<ul style="list-style-type: none"> TCFD-aligned disclosure Disclosure of Scope 1/2 (and 3 if appropriate) GHG emissions & reduction targets Enhanced disclosure for carbon-intensive industries 	<ul style="list-style-type: none"> Disclosure of HCM approach and link to strategy; comp & benefits, engagement, and DEI efforts and targets Disclosure of EEO-1 report 	<ul style="list-style-type: none"> Disclosure of board oversight of climate-related, HCM, and D&I risks & opportunities
	<ul style="list-style-type: none"> Suggests use of investor-aligned frameworks like ISSB 		<ul style="list-style-type: none"> Will hold directors accountable for material failures of risk oversight related to E&S issues

Stakeholder Expectations

Shareholder Proposals

- Basic idea: SEC rules allow shareholders of public companies to submit proposals to be voted on at the annual shareholders meeting and included in the company's proxy materials if certain conditions are met, including satisfying low stock ownership thresholds (\$2k-\$25k, depending on holding period)
- Why it matters: proposals are non-binding, but those receiving majority support or even significant minority support can trigger proxy advisor / investor board responsiveness policies where they may vote against directors if company response not deemed sufficient
- Trends in recent years: proposals historically focused on traditional governance issues (e.g., classified board), but in recent years there's been focus on environmental and social topics (including anti-ESG topics)
- Key stats over last 3 years:
 - >50% of all proposals submitted focused on E&S issues in each year
 - ~30 E&S proposals received majority support (but overall declining support for E&S)
 - #1 climate change was the most popular proposal topic in each year

Environmental Topics

- Climate reporting, lobbying, risks, transition planning, GHG goals
- Plastics, recycling, packaging
- Renewable energy
- Environmental impact

Social Topics

- Discrimination and diversity issues (e.g., racial equity audits)
- Employment, compensation & workplace issues (e.g., pay gap)
- Societal issues (e.g., human rights, animal welfare)

Governance Topics

- Independent board leadership
- Shareholder rights (e.g., special meetings, majority voting)
- Executive compensation issues
- Political contributions & lobbying activities

So Now What?

07

Task List

Key Governance Action Items to Get Ready for the IPO

- ✓ **Assemble public company board:** identify qualified independent directors and establish required board committees
- ✓ **Decide on important structural points,** including positioning generally on governance issues, board oversight structure & shareholder rights
- ✓ **Draft key documents:** certificate of incorporation, bylaws, governance guidelines, committee charters, code of conduct and other policies
- ✓ **Identify executive officers** who will be subject to public company restrictions (e.g., clawback, loan prohibition) and public disclosures (e.g., biographical, compensation, stock ownership, related party transactions)
- ✓ **Protect directors & officers** by adopting exculpation provisions, entering into indemnification agreements, purchasing D&O insurance
- ✓ **Build out key public company functions:** financial/SEC reporting, investor relations, public relations, internal audit, compliance, sustainability
- ✓ **Establish & augment controls:** disclosure controls and procedures, internal control over financial reporting, controls for voluntary disclosures
- ✓ **Consider other regulatory requirements & relevant stakeholder preferences,** as applicable
- ✓ **Don't forget about other tasks:** e.g., select state and exchange, build-out IR website, consider a board portal, identify a compensation consultant, etc.

Speaker Bios

08



Aaron Briggs

Partner / San Francisco

One Embarcadero Center, Suite 2600, San Francisco, CA 94111-3715

+1 415.393.8297

abriggs@gibsondunn.com

Aaron Briggs is a partner in Gibson Dunn’s San Francisco, CA office, where he works in the firm’s Securities Regulation & Corporate Governance practice group. Mr. Briggs’ practice focuses on advising public companies of all sizes (from pre-IPO to mega-cap), with a focus on technology and life sciences companies, on a wide range of securities and governance matters.

Before rejoining Gibson Dunn, Mr. Briggs served for five years as Executive Counsel - Corporate, Securities & Finance, at General Electric Company. His in-house experience—which included responsibility for SEC reporting and compliance, board governance, proxy and annual meeting, investor outreach and executive compensation matters, and included driving GE’s revamp of its full suite of investor communications (proxy statement, 10-K, earnings releases, and integrated report)—provides a unique insight and practical perspective on the issues that his clients face every day.

In 2023, Mr. Briggs was elected a Fellow of the American College of Governance Counsel, an organization of leading corporate governance lawyers from the US and Canada, and was inducted into the *Governance Intelligence* Hall of Fame. In 2016, *Corporate Secretary Magazine* named Mr. Briggs Governance Professional of the Year. Mr. Briggs’ work has also been recognized by Financial Executives International, ReportWatch, Sustainability Investment Leadership Council, and TheCorporateCounsel.net.

Mr. Briggs serves as Co-Chair of the Certified Corporate Governance Professional Oversight Commission for the Society for Corporate Governance and has been named a Transparency Advocate by RealTransparentDisclosure.com.

Mr. Briggs received his Juris Doctorate from the University of Chicago Law School in 2007, where he was a Kosmerl Scholar. He received his Bachelor of Arts with high honors from the University of Notre Dame in 2004.

EDUCATION

University of Chicago
Juris Doctor

University of Notre Dame
Bachelor of Arts



Hillary H. Holmes

Partner / Houston

811 Main Street, Suite 3000, Houston, TX 77002-6117

+1 346.718.6602

hholmes@gibsondunn.com

Hillary Holmes is Co-Chair of the firm's Capital Markets practice group and a member of the firm's Securities Regulation & Corporate Governance, Mergers & Acquisitions, and Energy & Infrastructure practice groups. Hillary also serves as co-partner-in-charge of the Houston office and as a member the firm's Executive Committee.

Hillary advises corporations, investment banks and institutional investors on long-term and strategic capital raising. She counsels boards of directors, special committees and financial advisors in M&A transactions, take privates and complex situations. She also regularly advises companies on securities laws, corporate governance and ESG issues. Hillary brings a deep expertise in the energy industry.

Chambers repeatedly ranks Hillary in the top tier for both energy capital markets and energy M&A / transactions, and as a premier lawyer for corporate counseling. *Law360* has twice selected her as an Energy MVP nationwide, *Hart Energy* named her one of the 25 Most Influential Women in Energy, *The National Law Journal* recognized her as a Capital Markets Trailblazer, *LawDragon 500* identifies her as a Leading Dealmaker in the US, *Texas Lawyer* named her a Most Effective Dealmaker and the Leading Woman in Energy, the *Houston Business Journal* named her a leading businesswoman, and her peers selected her as Corporate Lawyer of the Year in Houston.

Hillary is a member of the American Bar Association's Corporate Laws Committee, an officer of the Houston Chapter of the Society for Corporate Governance, an editor of Insights – The Corporate & Securities Law Advisor, a member of the Executive Council of the KBH Energy Center at the University of Texas, among other leadership positions.

Hillary received his Juris Doctorate from the University of Pennsylvania Law School in 2003, where she also received a Certificate in Public Policy from the Wharton School. She received her Bachelor of Arts, cum laude, from Duke University in 2003.

EDUCATION

University of Pennsylvania
Juris Doctor

Duke University
Bachelor of Arts



Lori Zyskowski

Partner / New York

200 Park Avenue, New York, NY 10166-0193

+1 212.351.2309

lzyskowski@gibsondunn.com

Lori Zyskowski is a partner in Gibson Dunn's New York office and Co-Chair of the firm's Securities Regulation & Corporate Governance practice group. Ms. Zyskowski advises public companies and their boards of directors on corporate governance matters, securities disclosure and compliance issues, shareholder engagement and activism matters, shareholder proposals, environmental, social and governance matters, and executive compensation practices.

Ms. Zyskowski advises clients, including public companies, their boards of directors, and board committees on corporate governance and securities disclosure matters, with a focus on fiduciary duties, oversight of enterprise risks, director independence, Securities and Exchange Commission reporting requirements, proxy statements, annual shareholders meetings, proxy advisory services, and executive compensation disclosure best practices. Ms. Zyskowski also advises on board succession planning and board evaluations and has considerable experience advising nonprofit organizations on governance matters. She was recognized as one of the 2024 *Lawdragon 500 Leading Dealmakers in America* and has been named by *Chambers USA* as a top Securities: Regulation attorney.

Before joining Gibson Dunn, for over a decade Ms. Zyskowski served as internal securities and corporate counsel at several large, publicly traded companies. Her in-house experience provides a unique insight and perspective on the issues that her clients face every day.

Ms. Zyskowski is a Fellow of the American College of Governance Counsel, an organization of leading corporate governance lawyers from the U.S. and Canada. She is a frequent speaker on governance, proxy and securities disclosure panels and is very active in the corporate governance community. She is a former member of the board of directors of the Society for Corporate Governance and previously served as the President of its New York Chapter.

She graduated from Columbia University School of Law in 1996 and was a Harlan Fiske Stone Scholar. Ms. Zyskowski received her undergraduate degree from Harvard University.

EDUCATION

Columbia University
Juris Doctor

Harvard University
Bachelor of Arts

GIBSON DUNN

GIBSON DUNN

2025 SEC Filing Deadlines

The calendar below reflects SEC filing deadlines for companies with a fiscal year ending December 31, 2024. For weekends and SEC holidays, the filing deadline is the next business day.

JANUARY						
Su	M	T	W	Th	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

FEBRUARY						
Su	M	T	W	Th	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	

MARCH						
Su	M	T	W	Th	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

APRIL						
Su	M	T	W	Th	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

MAY						
Su	M	T	W	Th	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

JUNE						
Su	M	T	W	Th	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

JULY						
Su	M	T	W	Th	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

AUGUST						
Su	M	T	W	Th	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

SEPTEMBER						
Su	M	T	W	Th	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

OCTOBER						
Su	M	T	W	Th	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

NOVEMBER						
Su	M	T	W	Th	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

DECEMBER						
Su	M	T	W	Th	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

-  Large Accelerated Filer
-  Accelerated Filer
-  Non-Accelerated Filer
-  Market Holidays (NYSE & Nasdaq)
-  Foreign Private Issuer
-  Proxy Statement
-  SEC Holiday
-  Market Early Close (1:00 PM EST)

Hours of EDGAR Operations: The hours of operation for submitting filings to the EDGAR system are 6:00 a.m. to 10:00 p.m. Eastern Time weekdays (excluding SEC holidays). If a filing is submitted after 5:30 p.m. Eastern Time, it will not be deemed filed with the SEC until the following business day (except for filings made pursuant to Rule 462(b), Section 16 filings and Schedule 13D/G filings, which will receive the date of the actual filing if filed by 10:00 pm Eastern Time).

Veteran's Day, Columbus Day and Good Friday: While trading remains open on Veteran's Day and Columbus Day, filing is unavailable. Filing is available on Good Friday, but the NYSE and NASDAQ are closed.

Periodic Report Filing Deadlines

Annual Report on Form 10-K	Large Accelerated Filer: 60 days after fiscal year end Accelerated Filer: 75 days after fiscal year end Non-Accelerated Filer: 90 days after fiscal year end
Quarterly Report on Form 10-Q	Large Accelerated Filer: 40 days after fiscal quarter end Accelerated Filer: 40 days after fiscal quarter end Non-Accelerated Filer: 45 days after fiscal quarter end
Annual Report on Form 20-F	For foreign private issuers, four months after fiscal year end
Definitive Proxy Statement	If Part III of Annual Report on Form 10-K incorporates by reference information from definitive proxy statement, 120 days after fiscal year end
“Glossy” Annual Report	Furnished through EDGAR no later than the date on which the report is first sent or given to shareholders

Ownership Reporting Deadlines

Form 3	10 days after becoming a director, officer or beneficial owner of more than 10% of a class of registered equity securities (or no later than the effective date of the registration statement if the issuer is registering equity for the first time)
Form 4	Two business days after the transaction date
Form 5	45 days after fiscal year end
Schedule 13G	Either 45 days after calendar quarter end or five business days after acquiring more than 5% beneficial ownership (depending on type of investor) (amendments generally due 45 days after calendar quarter end in which a material change occurs)
Schedule 13D	Five business days after acquiring more than 5% beneficial ownership (amendments due two business days after any material change)
Form 13F	45 days after each calendar quarter ends
Form N-PX	No later than August 31 of each year (which for 2025 will be August 29, 2025)

Other SEC Filing Deadlines

Form 8-K

Generally four business days after the occurrence of a triggering event, except for certain events as provided in the Form

Form SD (Conflict Minerals)

No later than May 31 of each year (which for 2025 will be May 30, 2025)

Form SD (Resource Extraction Issuers)

No later than 270 days after fiscal year end (which for companies with a fiscal year ending December 31, 2024, will be September 26, 2025)

Form 11-K

90 days after the employee plan's fiscal year end; if the employee plan is subject to ERISA, then 180 days after the employee plan's fiscal year end

Form 40-F

For Canadian foreign private issuers qualifying for the multi-jurisdictional disclosure system, then due the same day as the issuer's annual report is due to be filed in Canada

Large Accelerated Filer: A reporting company that has a public float of at least \$700 million, has been subject to the periodic reporting requirements of the Securities Exchange Act of 1934 ("1934 Act") for at least 12 months, has filed at least one annual report, and does not qualify as a smaller reporting company under the revenue test.

Accelerated Filer: A reporting company that has a public float of at least \$75 million but less than \$700 million, has been subject to the periodic reporting requirements of the 1934 Act for at least 12 months, and has filed at least one annual report, and does not qualify as a smaller reporting company under the revenue test.

Non-Accelerated Filer: A reporting company that has a public float of less than \$75 million, has not been subject to the periodic reporting requirements of the 1934 Act for more than 12 months, or has not filed at least one annual report.

Smaller Reporting Company: A reporting company that has (i) a public float of less than \$250 million or (ii) a public float of less than \$700 million (including having no public float) and annual revenues of less than \$100 million. An issuer cannot qualify as a smaller reporting company if it is an investment company, asset-backed issuer, or a majority-owned subsidiary of a parent that is not a smaller reporting company.

Public float is measured at end of second fiscal quarter, with any change in filing status taking effect as of the next fiscal year. Note thresholds transitioning between filer status categories are lower than those shown.

2025 Financial Statements Staleness Dates

Financial statements are considered “stale” when they are too old to be used in a prospectus or proxy statement. If an issuer’s financial statements have gone stale, the issuer must file the most recent required financial statements before using a prospectus or proxy statement. The table below reflects the staleness date, or the last date such financial statements may be used. For weekends and SEC holidays, the staleness date is the next business day.

Financial Statements	Deadline	2025 Staleness Date
Third quarter 2024 financial statements for initial public offerings, delinquent filers and loss corporations ¹	45 days after fiscal year end	February 14
Third quarter 2024 financial statements for large accelerated filers	60 days after fiscal year end	March 3
Third quarter 2024 financial statements for accelerated filers	75 days after fiscal year end	March 17
Third quarter 2024 financial statements for all other filers	90 days after fiscal year end	March 31
Year end 2024 financial statements for large accelerated filers and accelerated filers	129 days after fiscal year end	May 9
Year end 2024 financial statements for all other filers	134 days after fiscal year end	May 14
First quarter 2025 financial statements for large accelerated filers and accelerated filers	129 days after fiscal first quarter end	August 7
First quarter 2025 financial statements for all other filers	134 days after fiscal first quarter end	August 12
Second quarter 2025 financial statements for large accelerated filers and accelerated filers	129 days after fiscal second quarter end	November 6
Second quarter 2025 financial statements for all other filers	134 days after fiscal second quarter end	November 12

¹ A “delinquent filer” is a company that files annual, quarterly and other reports pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 but has not filed all reports due to be filed. A “loss corporation” is a company that does not expect to, and did not, report positive income after taxes but before extraordinary items and the cumulative effect of a change in accounting principle for (a) the most recently ended fiscal year and (b) at least one of the two prior fiscal years.

Note regarding Foreign Private Issuers:

Audited financial statements of a foreign private issuer go stale 15 months after the fiscal year end covered by such financial statements, and interim financial statements go stale nine months after the end of the period covered by such interim financial statements (for certain offerings, the 15-month period may be extended to 18 months, and the nine-month period may be extended to 12 months). If financial information for an annual or interim period more current than otherwise required is made available in any jurisdiction, such financial information should be included in the applicable registration statement.

For more information about current developments and trends in securities regulation, corporate governance and executive compensation, please see Gibson Dunn's [Securities Regulation and Corporate Governance Monitor](#).

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding the matters described above. Please contact the Gibson Dunn lawyer with whom you usually work in the firm's [Capital Markets](#) or [Securities Regulation and Corporate Governance](#) practice groups or any member of the Gibson Dunn team.

Please also feel free to contact any of the following practice leaders:

Capital Markets Group:

[Andrew L. Fabens](#) - New York (+1 212-351-4034, afabens@gibsondunn.com)

[Hillary H. Holmes](#) - Houston (+1 346-718-6602, hholmes@gibsondunn.com)

[Stewart L. McDowell](#) - San Francisco (+1 415-393-8322, smcdowell@gibsondunn.com)

[Peter W. Wardle](#) - Los Angeles (+1 213-229-7242, pwardle@gibsondunn.com)

Securities Regulation and Corporate Governance Group:

[Elizabeth A. Ising](#) - Washington, D.C. (+1 202-955-8287, eising@gibsondunn.com)

[James J. Moloney](#) - Orange County, CA (+1 949-451-4343, jmoloney@gibsondunn.com)

[Lori Zyskowski](#) - New York (+1 212-351-2309, lzyskowski@gibsondunn.com)

GIBSON DUNN



Fifth Circuit – Securities and Administrative Law
Update

July 1, 2024

Fifth Circuit Finds SEC’s “About-Face” On Proxy-Firm Disclosure Rule Arbitrary And Capricious

National Association of Manufacturers v. SEC, No. 22-51069 – Decided June 26, 2024

A unanimous Fifth Circuit panel vacated the SEC’s 2022 rescission of its 2020 proxy firm disclosure rule because the SEC failed to explain why the factual findings that supported the 2020 Rule were incorrect.

“[T]he SEC acted arbitrarily and capriciously in two ways. First, the agency failed adequately to explain its decision to disregard its prior factual finding that the notice-and-awareness conditions posed little or no risk to the timeliness and independence of proxy voting advice. Second, the agency failed to provide a reasonable explanation why these risks were so significant under the 2020 Rule as to justify its rescission.”

JUDGE JONES, WRITING FOR THE COURT

Background:

Shareholders of public companies are generally permitted under state law and SEC rules to vote on a variety of corporate-governance issues during shareholder meetings. Most shareholders do not attend these meetings in person, so they cast their votes by proxy. Institutional investors, who own a sizeable percentage of public company stock, vote in thousands of these meetings. They often retain proxy firms, such as Institutional Shareholder Services and Glass Lewis, to provide research and to advise them on how to vote.

SEC rules relating to proxy regulations, among other things, prohibit persons who solicit proxies from making misstatements or omissions of material fact in their solicitations and require such persons to furnish the targets of their solicitations with proxy statements containing certain disclosures. But proxy firms are also eligible for exemptions from these rules if they comply with certain conditions, and the business models of proxy firms rely on the availability of such exemptions.

Over the years, as proxy advisors grew in influence, however, concerns emerged about their practices. The proxy advisor market is “effectively a duopoly, because two firms . . . control roughly 97% of the market,” and “[i]nvestors, registrants, and others” began questioning the “accuracy of the information and the soundness of the advice that proxy firms provide” to shareholders and complaining about potential conflicts of interest and “the proxy firms’ unwillingness to engage with issuers to correct errors.” *Nat’l Ass’n of Manufacturers v. SEC*, No. 22-51069, 2024 WL 3175755, at *1 (5th Cir. June 26, 2024).

To address these and other concerns, the SEC undertook “nearly ten years of study and collaboration with all interested parties spanning two presidential administrations.” *Id.* at *2. This effort culminated in 2019, with the SEC’s proposal of a new rule that imposed additional conditions on the availability of exemptions for proxy firms. Importantly, amongst other requirements, the proposal required that proxy firms “provide registrants”—including public companies—“time to review and provide feedback on the advice **before** it is disseminated to the proxy firm’s clients.” *Id.* (cleaned up) (emphasis added). The rule’s purpose was to ensure the reliability and accuracy of the proxy firms’ advice by allowing a registrant an opportunity to correct any inaccuracies before dissemination. During the SEC’s 60-day comment period, however, some commentators expressed concern that the rule would delay and undermine the independence of the proxy firms’ advice.

When it adopted the rule in 2020 (the “[2020 Rule](#)”), the SEC addressed those concerns by requiring proxy firms (1) to provide their advice to registrants “**at or prior to**” the time they give their advice to their clients and (2) to allow their clients to see any written statements the registrant provided about the advice before the shareholder meeting. *Id.* at *3 (emphasis in original). Between the time the SEC finalized the rule and the date that proxy firms were required to comply with the new conditions, there entered a new SEC administration.

In November 2021, after all the SEC’s collaboration and deliberation, and just days before proxy firms were required to comply with the 2020 Rule, the new administration of the SEC published its proposal to rescind the 2020 Rule. It did so only after the new SEC chairman took office, held a closed-door meeting with the opponents of the 2020 Rule, suspended its enforcement, and directed his staff to reconsider the regulation in full. In July 2022, over the dissent of two

commissioners, the SEC formally rescinded the 2020 Rule, citing the same “timeliness” and “independence” concerns that the agency previously concluded the 2020 Rule was designed to address—all without explaining its change in position. *Id.* at *4.

Issue:

Is it arbitrary and capricious for an agency to reject its previous factual findings without explaining why those findings were incorrect?

Court's Holding:

Yes. An agency must provide a detailed explanation when rejecting prior factual findings.

What It Means:

- The Fifth Circuit’s decision makes clear that, although a new administration may rescind prior rules, the agency must adequately explain any departure from its prior factual findings. Litigants seeking to challenge an agency’s flip-flop should pay careful attention to the agency’s justification for the change—particularly when it involves contradicting prior agency fact finding.
- The Fifth Circuit’s decision also underscores courts’ refusal to credit agency litigation positions or other post hoc rationalizations for an agency’s change in position: “[I]n reviewing an agency’s action, we may consider only the reasoning articulated by the agency itself; we cannot consider *post hoc* rationalizations.” *Id.* at *8 (cleaned up).
- The Fifth Circuit also confirmed that the “default” remedy when “an agency rule violates the APA” is “vacatur”—indeed, a court “shall—not may—hold unlawful and set aside [such] agency action.” *Id.* at *9 (cleaned up). Accordingly, successful challenges to any agency’s rule will generally result in the rule being set aside.
- This case was one of many challenges relating to SEC rulemaking regarding the regulation of proxy advisory firms. For instance, the D.C. District Court recently held, regarding another part of the 2020 Rule defining “solicit,” that “the SEC acted contrary to law and in excess of statutory authority when it amended the proxy rules’ definition of ‘solicit’ and ‘solicitation’ to include proxy voting advice for a fee.” *ISS Inc. v. SEC*, No. 19-CV-3275, 2024 WL 756783, at *2 (D.D.C. Feb. 23, 2024), *notices of appeal filed*, Nos. 24-5105, 24-5112 (D.C. Cir.). And the Western District of Texas previously held that the SEC’s suspension of the 2020 Rule was unlawful because it was done without notice and comment. *NAM v. SEC*, 631 F. Supp. 3d 423 (W.D. Tex. 2022).
- Future SEC rules directed at proxy firms will likely continue to face challenges in court. The proxy advisor industry is also likely to continue to face challenges over the issues that led to the 2020 Rule. Moreover, corporations, investors, and proxy advisors will need to work to address these concerns in an often politicized corporate governance environment.

Gibson Dunn Appellate Honors



The Court's opinion is available [here](#).

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding developments at the U.S. Supreme Court. Please feel free to contact the following practice group leaders:

Related Practice: Securities Enforcement

[Mark K. Schonfeld](#)

+1 212.351.2433

mschonfeld@gibsondunn.com

[David Woodcock](#)

+1 214.698.3211

dwoodcock@gibsondunn.com

Related Practice: Securities Regulation and Corporate Governance

[Elizabeth A. Ising](#)

+1 202.955.8287

eising@gibsondunn.com

[James J. Moloney](#)

+1 949.451.4343

jmoloney@gibsondunn.com

[Lori Zyskowski](#)

+1 212.351.2309

lzyskowski@gibsondunn.com

Related Practice: Administrative Law and Regulatory Practice

[Eugene Scalia](#)

+1 202.955.8210

escalia@gibsondunn.com

[Helgi C. Walker](#)

+1 202.887.3599

hwalker@gibsondunn.com

[Stuart F. Delery](#)

+1 202.955.8515

sdelery@gibsondunn.com

Related Practice: Securities Litigation

[Monica K. Loseman](#)

+1 303.298.5784

mloseman@gibsondunn.com

[Brian M. Lutz](#)

+1 415.393.8379

blutz@gibsondunn.com

[Craig Varnen](#)

+1 213.229.7922

cvarnen@gibsondunn.com

Related Practice: Appellate and Constitutional Law

Thomas H. Dupree Jr.
+1 202.955.8547
tdupree@gibsondunn.com

Allyson N. Ho
+1 214.698.3233
aho@gibsondunn.com

Julian W. Poon
+1 213.229.7758
jpoon@gibsondunn.com

Brad G. Hubbard
+1 214.698.3326
bhubbard@gibsondunn.com

This alert was prepared by associates Brian Richman, Elizabeth A. Kiernan, and Brian Sanders.

Attorney Advertising: These materials were prepared for general informational purposes only based on information available at the time of publication and are not intended as, do not constitute, and should not be relied upon as, legal advice or a legal opinion on any specific facts or circumstances. Gibson Dunn (and its affiliates, attorneys, and employees) shall not have any liability in connection with any use of these materials. The sharing of these materials does not establish an attorney-client relationship with the recipient and should not be relied upon as an alternative for advice from qualified counsel. Please note that facts and circumstances may vary, and prior results do not guarantee a similar outcome.

If you would prefer NOT to receive future emailings such as this from the firm,
please reply to this email with "Unsubscribe" in the subject line.

If you would prefer to be removed from ALL of our email lists,
please reply to this email with "Unsubscribe All" in the subject line. Thank you.

© 2024 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at gibsondunn.com

GIBSON DUNN



**Capital Markets and Securities Regulation &
Corporate Governance Update**

September 10, 2024

Early Insights from Insider Trading Policies Filed by S&P 500 Companies under the SEC’s New Exhibit Requirement

I. Introduction

For fiscal years beginning on or after April 1, 2023, domestic public companies are required to disclose whether they have adopted insider trading policies and procedures governing the purchase, sale, and/or other dispositions of their securities by their directors, officers and employees, or the companies themselves, and if so to file those policies and procedures as an exhibit to their annual reports on Form 10-K.^[1] While calendar year companies must comply with these requirements in their Form 10-K for, or proxy statement following, the fiscal year ending December 31, 2024, 49 S&P 500 companies had addressed these requirements in filings as of June 30, 2024.^[2]

As discussed in the summary of our preliminary observations below, while specific provisions vary from company to company, certain common approaches are emerging with respect to key policy terms. That said, company policies and procedures can vary based on a company’s particular circumstances, some companies may have interpretive materials that were not filed but elaborate on the operation of their policies and procedures, and some companies are updating their policies and procedures in light of the new filing requirements. As a result, we caution companies against treating these early observations as “best practices.” Your Gibson Dunn

contacts are available to discuss the specifics of your policy and answer any questions you may have.

II. Persons Subject to the Insider Trading Policies

Nearly all policies we reviewed (96%) cover all company personnel (i.e., directors, officers and all employees of companies and their subsidiaries and, in some cases, certain affiliates) and their family members. Additionally, a significant majority of the policies (82%) expressly state that they apply to legal entities such as trusts whose securities transactions are controlled or influenced by company personnel and, in some cases, their family members. A majority of the policies (63%) also apply insider trading restrictions to contractors and/or consultants.^[3]

III. Transactions in Company Securities Subject to the Insider Trading Policies

All of the policies specify types of transactions that are subject to, or are exempt from, the policy terms. Aside from open market sales or purchases, which are addressed in all of the policies, the most commonly addressed transactions include the following:

- A significant majority of the policies (86%) provide some level of restriction on gifts, addressing to one degree or another the SEC's position that gifts can constitute a form of insider trading.^[4] A majority (61%) specifically address gifts as being subject to the policy for all covered persons (i.e., prohibiting gifts when an individual subject to the policy is in possession of material nonpublic information ("MNPI") and/or applying window periods and/or pre-clearance restrictions to gifts),^[5] although a handful of companies (8%) restrict gifts only if the donor has reason to believe the donee will sell while the donor has MNPI. Of the policies that do not apply gift restrictions to all employees, a majority restrict gifts only for certain covered persons that are subject to additional restrictions, such as blackout periods and/or pre-clearance procedures.
- *Option Exercises.* A majority of the policies (69%) exempt exercises of options when there is no associated sale on the market; however, exercises of options where there is a sale of some or a portion of shares delivered upon exercise (e.g., cashless broker exercise) are typically treated like any other sale. Of this group, approximately a quarter of the policies specifically provide that withholding of shares for tax withholding purposes is exempt, and a smaller minority of policies provide that withholding of shares for tax withholding purposes and/or the payment of exercise price is exempt.
- *Vesting and Settlement of Other Equity Awards.* A majority of the policies (59%) exempt vesting and settlement of equity awards, such as RSUs and restricted stock, and 51% of the policies specifically provide that withholding of shares for tax purposes (i.e., net share settlement) is exempt.

IV. Transactions in Other Company Securities

Nearly all policies (96%) specifically include some form of restriction on trading in the securities of another company when the person is aware of MNPI about that company or its securities. A significant majority of the policies (82%) prohibit trading in the securities of another company when the person is aware of MNPI about such company that was learned in the course of or as a result of the covered person's employment or relationship with the company. The rest apply the prohibition more broadly to trading in the securities of another company while aware of MNPI

about that company, without specifically addressing how the information was learned. Of the 82%, a minority tailor the prohibition to apply only to trading in the securities of another company that has some sort of a business relationship with the company (e.g., customers, vendors, or suppliers) or that is engaged in a potential business transaction with the company, and a smaller subset of these policies also include a specific reference to “competitors” in this prohibition.

V. Blackout Periods and Preclearance Procedures

- *Persons subject to quarterly blackout periods.* A significant majority of the policies (88%) subject directors, executive officers and a designated subset of employees to regular quarterly blackout periods, with a few policies applying two different blackout periods to different groups of employees. Although the groups of persons (other than directors and executive officers) who are subject to quarterly blackout periods tend to be company-specific, most of the policies identify the “restricted persons” to include employees by title (e.g., all Vice Presidents or higher) and/or by department or role (e.g., all officers in accounting, financial planning and analysis, investor relations, legal and finance departments, etc.) as well as other employees who have been identified as having access to systems that have MNPI. Some policies take a less specific approach and identify restricted persons as those who are designated as such by the officer administering the insider trading policy. A minority of the policies (6%) subject all covered persons under the policy to quarterly blackout periods.
- *Start and end of quarterly blackout periods.* The start date of the quarterly blackout periods ranges from quarter end to four weeks or more prior to quarter end. Under almost half of the policies (45%), the quarterly blackout periods start approximately two weeks prior to quarter end, 14% start the blackout periods three to four weeks prior to quarter end, and 18% start four weeks or more prior to quarter end. A significant majority of the policies (76%) end the quarterly blackout periods one to two full trading days after the release of earnings, with more policies ending after one trading day (51%) than two trading days (24%).^[6] Additionally, nearly all policies specifically state that from time to time the company may implement additional special blackout periods.
- *Preclearance procedures.* Nearly all policies require that certain covered persons must preclear their transactions with the appropriate officer administering the insider trading policy prior to execution. There is, however, variation in the persons subject to preclearance procedures—for 65% of the policies, the preclearance persons are a subset of the persons subject to blackout periods, while for a minority of the policies (29%), they are the same as the persons subject to the blackout periods. Of the 65% of the policies, a minority (38%) require preclearance only from the company’s directors and executive officers.^[7] Regardless of scope, nearly all of the policies provide that directors and executive officers are subject to preclearance procedures.

VI. Special Prohibitions Under the Insider Trading Policies

All of the policies prohibit or otherwise restrict certain types of transactions regardless of whether they involve actual insider trading, in some cases stating that such transactions present a heightened risk of securities law violations or the potential appearance of improper or inappropriate conduct. The most common prohibitions addressed: hedging transactions (96%);^[8] speculative transactions (96%); pledging securities as collateral for a loan (90%); and trading on margin or holding securities in margin accounts (82%). Although a significant majority of the policies apply the prohibition on hedging and speculative transactions to all persons subject to the

policy, prohibitions on pledging and/or margin trading/accounts are sometimes limited to sub-categories of persons subject to the insider trading policies (39% and 27%, respectively): for instance, some policies apply the prohibition only to directors and executive officers or persons subject to quarterly blackout periods and/or preclearance procedures.^[9]

A significant majority of the policies do not specifically address standing or limit orders or short-term trading, but of the ones that do, a significant majority take the approach of discouraging such transactions rather than strictly prohibiting them. Even where standing or limit orders are not strictly prohibited, some policies require that such orders be cancelled if the person becomes aware of MNPI (or prior to the start of a blackout period, if applicable). A few policies prohibit standing or limit orders if they go beyond a specified duration.

VII. Rule 10b5-1 Plans

All of the policies address the availability of Rule 10b5-1 plans. A significant majority of the policies (86%) do not set forth restrictions on who can enter into a Rule 10b5-1 plan so long as approval and other requirements are met, but a minority of the policies (12%) limit the use of 10b5-1 plans to directors and designated officers. A small minority of the policies (6%) require directors and designated officers to trade only pursuant to Rule 10b5-1 plans.

All of the policies require that Rule 10b5-1 plans be approved prior to adoption, but the policies tend to vary in approach when describing the guidelines for entering into Rule 10b5-1 plans (or modifying or terminating them). A significant majority (71%) of the policies describe the specified conditions under the SEC rules for a plan to qualify as a Rule 10b5-1 plan, although some do so in a more streamlined manner than others. Of these policies, a majority include Rule 10b5-1 plan requirements within the body of the policy, although a minority do so in an appendix and one company filed the plan guidelines as a separate exhibit. A minority of the policies (29%) do not describe the specified conditions under Rule 10b5-1, but provide a general statement regarding the affirmative defense from insider trading liability under the securities laws for transactions under a compliant Rule 10b5-1 plan and refer covered persons to the officer administering the policy for more information and guidelines on how to establish such a plan.

VIII. Policies Addressing Company Transactions

As noted above, Item 408(b) of Regulation S-K requires a public company to disclose whether it has adopted insider trading policies and procedures governing transactions in company securities by the company itself, and, if so, to file the policies and procedures, or if not, to explain why. Of the 23 S&P 500 companies subject to Item 408(b) that filed a Form 10-K and proxy statement prior to June 30, 2024, a significant majority (78%) did not address insider trading policies or procedures governing companies' transactions in their own securities.^[10] Of the ones that did, most included a brief sentence or two about the company's policy of complying with applicable laws in trading in its own securities. Only one company in our surveyed group filed a company repurchase policy as a separate exhibit.

IX. Filing Practices Regarding Related Policies or Documents

A significant majority (88%) of the companies filed only a single insider trading policy and no other related policies or documents (even where they referenced other related policies in their insider trading policy).^[11] In the few cases where multiple policies were filed, they appear to be supplemental guidelines/policies covering topics not generally applicable to all employees (e.g., trading windows, preclearance, 10b5-1 plans).

* * * *

We will continue to monitor public company filings of insider trading policies and procedures and expect to update our survey in early 2025 once calendar year-end companies' Forms 10-K are on file, as we expect disclosure and filing practices to evolve as companies go through the first full year of complying with the new Item 408(b) disclosure and filing requirements.

^[1] See Items 408(b) and 601(b)(19) of Regulation S-K, adopted by the SEC in connection with the Rule 10b5-1 amendments in December 2022. If a company has not adopted such policies and procedures, it is required to explain why it has not done so. Disclosure about the adoption (or not) of policies or procedures must appear in a company's proxy statement (and must also be included in, or incorporated by reference to, Part III of a company's Form 10-K), whereas the policies and procedures are to be filed as exhibits to the company's Form 10-K.

^[2] This group of 49 S&P 500 companies includes 23 companies that made Item 408(b) disclosures and 26 companies that were not subject to the disclosure requirements but voluntarily filed their insider trading policies and procedures with a Form 10-K filed prior to June 30, 2024.

^[3] A minority of policies also include other service providers specific to their businesses.

^[4] See Final Rule: Insider Trading Arrangements and Related Disclosures, [Release No. 33-11138](#) (Dec. 14, 2022). In its adopting release, the SEC stated its view that the terms "trade" and "sale" in Rule 10b5-1 include bona fide gifts of securities and that gifts can be subject to Section 10(b) liability, since the Securities Exchange Act of 1934 does not require that a "sale" be for value and instead provides that the terms "sale" or "sell" each include "any contract to sell or otherwise dispose of."

^[5] A small minority of these policies also provide certain exceptions for gifts, including gifts to family members and/or controlled entities that are already subject to the policy, or exceptions on a case by case basis.

^[6] Some policies use business days instead of trading days, but many policies do not define either term. We treated them as the same for purposes of our data analysis.

^[7] The remaining 6% includes two policies that do not address preclearance procedures and one policy which is unclear.

^[8] Item 407(i) of Regulation S-K requires companies to disclose practices or policies they have adopted regarding the ability of employees (including officers) or directors to engage in certain hedging transactions.

[9] A few policies allow for exceptions, subject to preclearance.

[10] For the purposes of this survey, we limited our review to Exhibit 19 filings and did not review the companies' disclosures in the body of the proxy statement or Form 10-K addressing Item 408(b)(1) of Regulation S-K.

[11] Under Regulation S-K Item 408(b)(2), if all of a company's insider trading policies and procedures are included in its code of ethics that is filed as an exhibit to the company's Form 10-K, that satisfies the exhibit requirement. However, many companies do not file their code of ethics and instead rely on one of the alternative means of making the code available allowed under S-K Item 406(c)(2) and (3).

The following Gibson Dunn lawyers assisted in preparing this update: Aaron K. Briggs, Thomas Kim, Brian Lane, Julia Lapitskaya, James Moloney, Ronald Mueller, Michael Titera, Lori Zyskowski, and Stella Kwak.

Gibson Dunn's lawyers are available to assist with any questions you may have regarding these developments. To learn more, please contact the Gibson Dunn lawyer with whom you usually work, or any leader or member of the firm's Capital Markets or Securities Regulation and Corporate Governance practice groups:

Capital Markets:

Andrew L. Fabens – New York (+1 212.351.4034, afabens@gibsondunn.com)

Hillary H. Holmes – Houston (+1 346.718.6602, hholmes@gibsondunn.com)

Stewart L. McDowell – San Francisco (+1 415.393.8322, smcdowell@gibsondunn.com)

Peter W. Wardle – Los Angeles (+1 213.229.7242, pwardle@gibsondunn.com)

Securities Regulation and Corporate Governance:

Elizabeth Ising – Washington, D.C. (+1 202.955.8287, eising@gibsondunn.com)

James J. Moloney – Orange County (+1 949.451.4343, jmoloney@gibsondunn.com)

Lori Zyskowski – New York (+1 212.351.2309, lzyskowski@gibsondunn.com)

Aaron Briggs – San Francisco (+1 415.393.8297, abriggs@gibsondunn.com)

Thomas J. Kim – Washington, D.C. (+1 202.887.3550, tkim@gibsondunn.com)

Brian J. Lane – Washington, D.C. (+1 202.887.3646, blane@gibsondunn.com)

Julia Lapitskaya – New York (+1 212.351.2354, jlapitskaya@gibsondunn.com)

Ronald O. Mueller – Washington, D.C. (+1 202.955.8671, rmueller@gibsondunn.com)

Michael Scanlon – Washington, D.C. (+1 202.887.3668, mscanlon@gibsondunn.com)

Mike Titera – Orange County (+1 949.451.4365, mtitera@gibsondunn.com)

Attorney Advertising: These materials were prepared for general informational purposes only based on information available at the time of publication and are not intended as, do not constitute, and should not be relied upon as, legal advice or a legal opinion on any specific facts or circumstances. Gibson Dunn (and its affiliates, attorneys, and employees) shall not have any liability in connection with any use of these materials. The sharing of these materials does not establish an attorney-client relationship with the recipient and should not be relied upon as an alternative for advice from qualified counsel. Please note that facts and circumstances may vary, and prior results do not guarantee a similar outcome.

If you would prefer NOT to receive future emailings such as this from the firm,
please reply to this email with "Unsubscribe" in the subject line.

If you would prefer to be removed from ALL of our email lists,
please reply to this email with "Unsubscribe All" in the subject line. Thank you.

© 2024 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at [gibsondunn.com](https://www.gibsondunn.com)

SEC Adopts Sweeping New Climate Disclosure Requirements for Public Companies

An Overview of the Highlights and Key Differences to the Proposed Rules

On March 6, 2024, the Securities and Exchange Commission (“SEC” or “Commission”), in a divided 3-2 vote along party lines, adopted final rules establishing climate-related disclosure requirements for U.S. public companies and foreign private issuers in their annual reports on Form 10-K and Form 20-F, as well as for companies looking to go public in their Securities Act registration statements. The Commission issued the [Proposing Release](#) in March 2022, which we previously summarized [here](#), and received more than 22,500 comments (including more than 4,500 unique letters) from a wide range of individuals and organizations. The Adopting Release is available [here](#) and a fact sheet from the SEC is available [here](#). A summary table discussing in more detail the notable changes between the Adopting Release and the Proposing Release is provided below.

We will provide more resources. Register [here](#) for Gibson Dunn's webcast covering key aspects of the final rules and litigation developments on Tuesday, March 12, 2024. Our review of the final rules and Adopting Release is ongoing. We will publish a revised and more detailed summary of the final rules and related topics.

Overview of the final rules. The final rules will require disclosure in annual reports and registration statements of:

- **Material impacts on operations.** How any climate-related risks have had, or are reasonably likely to have, material impacts on a company's results of operations, strategy, or financial condition.
- **Impact on the company.** How any such climate-related risks have materially affected or are reasonably likely to materially affect a company's outlook, strategy, and business model, as well as a new financial statement note reporting expenditures and costs above a de minimis threshold resulting from severe weather events, other “natural conditions,” and certain carbon offsets and renewable energy certificates (“REC”).
- **Risk management/oversight process.** Board and management governance and practices related to climate-related risk identification, assessment, management, and oversight.
- **GHG emissions and assurance.** Scope 1 and Scope 2 greenhouse gas (“GHG”) emissions, if material, for accelerated and large accelerated filers only, with phased-in assurance by an independent GHG emissions attestation provider.
- **Targets/goals.** Information regarding climate-related targets or goals that have materially affected, or are reasonably likely to materially affect, the company's results of operations, business, or financial condition.

GIBSON DUNN

- **Mitigation efforts.** Transition plans to address material transition risks, scenario analyses used for assessing material climate-related risk impacts, and internal carbon pricing if its use is material to managing material climate-related risks.

Significant changes from the rule proposal. The Commission made several notable changes to the proposed requirements, including to:

- eliminate Scope 3 GHG emissions reporting requirements;
- limit the requirement to report Scope 1 and 2 GHG emissions only if material, and exempt non-accelerated filers, smaller reporting companies and emerging growth companies from emissions reporting;
- prolong the phase-in period for third-party assurance requirements for emissions reporting, and require only large accelerated filers to eventually (by 2033) obtain attestation at a “reasonable assurance” level;
- remove the requirement to disclose directors’ climate-related expertise;
- limit the Regulation S-X (“Reg. S-X”) financial footnote requirement to (1) expenditures, charges, and losses incurred as a result of severe weather events and other natural conditions that are 1% or more of either net income before tax and/or stockholders’ equity, depending on whether such amounts are expensed or capitalized, and (2) carbon offsets and renewable energy credits that are a material component of a company’s plan to achieve its disclosed climate-related targets or goals; and
- adopt a new requirement to disclose, outside of the financial statements, the amount of material expenditures incurred as a result of any transition plan.

More broadly, the final rules adopt “materiality” qualifiers for many of the disclosure requirements, and the number of prescriptive disclosure requirements has been reduced. The preamble to the final rules also states that “traditional” notions of “materiality” will apply, as defined in Supreme Court precedents. Notwithstanding these changes, the final rules impose a significant reporting burden on companies and require substantial planning to prepare to comply.

Compliance phase-in period. The final rules will become effective 60 days after publication in the Federal Register (available [here](#)). The requirement to comply with the final rules will phase in over time, based on a company’s filer status. Registration statements will be subject to these disclosure obligations based on the fiscal years being reported. The first required disclosures for U.S. public companies with a calendar-end fiscal year will begin with the annual report on Form 10-K filed in:

Disclosure Requirement	Large Accelerated Filers	Accelerated Filers*	Non-Accelerated Filers / Smaller Reporting Companies / Emerging Growth Companies
Reg. S-K & Reg. S-X requirements other than:	<u>2026</u> for FY 2025	<u>2027</u> for FY 2026	<u>2028</u> for FY 2027
Certain quantitative & qualitative disclosures under Items 1502(d)(2), 1502(e)(2), & 1504(c)(2)	<u>2027</u> for FY 2026	<u>2028</u> for FY 2027	<u>2029</u> for FY 2028
Scopes 1 & 2 GHG Emissions**	<u>2027</u> for FY 2026	<u>2029</u> for FY 2028	N/A
Limited Assurance of GHG Emissions	<u>2030</u> for FY 2029	<u>2032</u> for FY 2031	N/A
Reasonable Assurance of GHG Emissions	<u>2034</u> for FY 2033	N/A	N/A
Inline XBRL Tagging for Reg. S-K Requirements***	<u>2027</u> for FY 2026	<u>2027</u> for FY 2026	<u>2028</u> for FY 2027

* This applies only to Accelerated Filers that are not also Smaller Reporting Companies or Emerging Growth Companies.

** Scope 1 & 2 GHG emissions for the most recent fiscal year may be reported as late as the second quarter Form 10-Q deadline.

*** Reg. S-X requirements will be tagged with the first disclosure.

Disclosure Category	Proposing Release Standards	Adopting Release Changes
<p>Climate-Related Risk Oversight & Management</p> <p><i>(Items 1501 & 1503, Reg. S-K)</i></p>	<p>Describe climate-related risk oversight and management, including the role of the board in overseeing and management in assessing and managing climate-related risks, and related risk management processes.</p>	<p>Adopted substantially as proposed.</p> <p><u>Notable Changes:</u></p> <ul style="list-style-type: none"> Removed several prescriptive disclosure requirements related to directors' climate-related expertise, board discussion and consideration of climate-related risks, board target setting, and board oversight of climate-related opportunities; added instruction providing examples of relevant management expertise to disclose; and focused on processes for identifying, assessing, and managing material climate-related risks.
<p>Climate-Related Risks and Impacts</p> <p><i>(Item 1502, Reg. S-K)</i></p>	<p>Describe material climate-related risks, including:</p> <ul style="list-style-type: none"> their impacts, timeframe, and nature, and how the company considers or incorporates them; the business strategy's resilience against changes in climate-related risks, including use of scenario analyses; and the company's transition plan(s) adopted for its management strategy for such risks, including relevant metrics, targets, and actions taken. 	<p>Adopted with significant revisions.</p> <p><u>Notable Changes:</u></p> <ul style="list-style-type: none"> Removed requirement to discuss business strategy resilience against changes in climate-related risks; revised to focus only on transition plans adopted for managing material transition risks (rather than those adopted within the company's climate-related risk management strategy); scenario analyses used for assessing material climate-related risk impacts to the company (rather than as a tool used for assessing business resilience); and internal carbon pricing material to evaluating and managing climate-related risks

GIBSON DUNN

Disclosure Category	Proposing Release Standards	Adopting Release Changes
		<p>(rather than any maintenance of an internal carbon price); and</p> <ul style="list-style-type: none"> removed requirement to discuss metrics and targets for the identification and management of transition and physical risks.
<p>GHG Emissions Reporting Disclosures</p> <p><i>(Items 1504 & 1505, Reg. S-K)</i></p>	<p>All companies must disclose Scope 1 and Scope 2 GHG emissions. All companies (except smaller reporting companies) must disclose Scope 3 GHG emissions if (i) material to the company or (ii) the company has set a GHG emissions target that includes Scope 3.</p> <p>Attestation is required for Scope 1 and Scope 2 for large accelerated and accelerated filers, subject to a phase in from limited assurance to reasonable assurance within two to four fiscal years after the compliance date. No attestation is required for Scope 3.</p>	<p>Adopted, with significant revisions, as Items 1505 & 1506.</p> <p><u>Notable Changes:</u></p> <ul style="list-style-type: none"> Eliminated Scope 3 GHG emissions disclosure requirements; limited Scope 1 and Scope 2 GHG emissions disclosure to large accelerated filers and accelerated filers, and only if material (e.g., to an investor’s voting or investment decision, or, if omitted, as significantly altering the total mix of information); delayed emissions reporting deadline for the most recent fiscal year to the second quarter Form 10-Q filing deadline (or 225 days after fiscal year end for Form 20-F or registration statement filers), instead of requiring inclusion in the annual report on Form 10-K (or Form 20-F); delayed “limited assurance” attestation requirement for Scope 1 and 2 GHG emissions until the third fiscal year after the compliance date; and limited requirement to transition to “reasonable assurance” attestation to large accelerated filers only, and

Disclosure Category	Proposing Release Standards	Adopting Release Changes
		extended phase-in to the seventh fiscal year after the compliance date.
<p>Targets, Goals & Transition Plans Disclosures</p> <p><i>(Item 1506, Reg. S-K)</i></p>	<p>Describe GHG emission or other climate-related targets or goals, including pathway to achievement, progress made, and use of carbon offsets or RECs.</p>	<p>Adopted, with some revisions, as Item 1504.</p> <p><u>Notable Changes:</u></p> <ul style="list-style-type: none"> Revised disclosure trigger to focus only on climate-related targets or goals that materially affect (or are reasonably likely to materially affect) the business, financial condition, or results of operations, rather than requiring disclosure whenever the company has set a GHG emissions reduction or other climate-related target or goal; and added disclosure requirements related to material impacts and expenditures from such targets or goals (or actions related thereto).
<p>Climate-Related Financial Statement Disclosure</p> <p><i>(Rules 14-01 and 14-02 of Reg. S-X)</i></p>	<p>Disclose (i) climate-related financial metrics related to the impacts of severe weather events and activities to reduce GHG emissions or exposure to transition risks if the absolute value of those impacts or expenditures/costs, as applicable, represents at least 1% of its corresponding financial statement line item and (ii) the impact of climate-related events on estimates and assumptions.</p> <p>Disclosures must be provided for the company's most recently completed fiscal year and for each historical fiscal year included in</p>	<p>Adopted with significant revisions.</p> <p><u>Notable Changes:</u></p> <ul style="list-style-type: none"> Replaced the requirement to disclose changes representing 1% of a line item with a new requirement to disclose aggregated cost and charges (and separately, recoveries) due to severe climate events and other natural conditions that exceed one percent of net income before tax or stockholders' equity, depending on whether such amounts are expensed or capitalized; replaced the requirement to disclose costs/expenditures for general

GIBSON DUNN

Disclosure Category	Proposing Release Standards	Adopting Release Changes
	the financial statements in the filing.	<p>transition activities and mitigating risks from climate-related events and conditions with a requirement to disclose whether any estimates/assumptions used in creating the consolidated financial statements had material impacts from climate-related targets or transition plans disclosed by the company (in addition to severe weather events or natural conditions); and</p> <ul style="list-style-type: none"> • added requirement to disclose expensed or capitalized carbon offsets and RECs if material to a company’s transition plan.

The following Gibson Dunn lawyers prepared this update: Aaron Briggs, Elizabeth Ising, Thomas Kim, Brian Lane, Julia Lapitskaya, Cynthia Mabry, Lori Zyskowski, Natalie Abshez, Lauren Assaf-Holmes, Spencer Bankhead, Irina Dykhne, Amanda Estep, Hannah Gonzalez, Chad Kang, Stefan Koller, Marie Kwon, Antony Nguyen, Andrea Shen, Meghan Sherley, Jack Strachan, and Maggie Valachovic.

Gibson, Dunn & Crutcher’s lawyers are available to assist in addressing any questions you may have about these developments. To learn more about these issues, please contact the Gibson Dunn lawyer with whom you usually work, or any of the following lawyers in the firm’s [Securities Regulation and Corporate Governance](#), [Environmental, Social and Governance \(ESG\)](#), [Capital Markets](#), [Administrative Law and Regulatory](#), and [Environmental Litigation and Mass Tort](#) practice groups:

Securities Regulation and Corporate Governance:

- [Elizabeth Ising](#) – Washington, D.C. (+1 202.955.8287, eising@gibsondunn.com)
- [James J. Moloney](#) – Orange County (+1 1149.451.4343, jmoloney@gibsondunn.com)
- [Lori Zyskowski](#) – New York (+1 212.351.2309, lzyskowski@gibsondunn.com)
- [Brian J. Lane](#) – Washington, D.C. (+1 202.887.3646, blane@gibsondunn.com)
- [Thomas J. Kim](#) – Washington, D.C. (+1 202.887.3550, tkim@gibsondunn.com)
- [Ronald O. Mueller](#) – Washington, D.C. (+1 202.955.8671, rmueller@gibsondunn.com)
- [Michael Scanlon](#) – Washington, D.C. (+1 202.887.3668, mscanlon@gibsondunn.com)

GIBSON DUNN

[Mike Titera](#) – Orange County (+1 1149.451.4365, mtitera@gibsondunn.com)
[Aaron Briggs](#) – San Francisco (+1 415.393.8297, abriggs@gibsondunn.com)
[Julia Lapitskaya](#) – New York (+1 212.351.2354, jlapitskaya@gibsondunn.com)

Environmental, Social and Governance (ESG):

[Susy Bullock](#) – London (+44 20 7071 4283, sbullock@gibsondunn.com)
[Elizabeth Ising](#) – Washington, D.C. (+1 202.955.8287, eising@gibsondunn.com)
[Perlette M. Jura](#) – Los Angeles (+1 213.229.7121, pjura@gibsondunn.com)
[Ronald Kirk](#) – Dallas (+1 214.698.3295, rkirk@gibsondunn.com)
[Cynthia M. Mabry](#) – Houston (+1 346.718.6614, cmabry@gibsondunn.com)
[Michael K. Murphy](#) – Washington, D.C. (+1 202.955.8238, mmurphy@gibsondunn.com)
[Selina S. Sagayam](#) – London (+44 20 7071 4263, ssagayam@gibsondunn.com)
[William E. Thomson](#) – Los Angeles (+1 213.229.7891, wthomson@gibsondunn.com)

Capital Markets:

[Andrew L. Fabens](#) – New York (+1 212.351.4034, afabens@gibsondunn.com)
[Hillary H. Holmes](#) – Houston (+1 346.718.6602, hholmes@gibsondunn.com)
[Stewart L. McDowell](#) – San Francisco (+1 415.393.8322, smcdowell@gibsondunn.com)
[Peter W. Wardle](#) – Los Angeles (+1 213.229.7242, pwardle@gibsondunn.com)

Administrative Law and Regulatory:

[Eugene Scalia](#) – Washington, D.C. (+1 202.955.8543, escalia@gibsondunn.com)
[Jonathan C. Bond](#) – Washington, D.C. (+1 202.887.3704, jbond@gibsondunn.com)

Environmental Litigation and Mass Tort:

[Stacie B. Fletcher](#) – Washington, D.C. (+1 202.887.3627, sfletcher@gibsondunn.com)
[Michael K. Murphy](#) – Washington, D.C. (+1 202.955.8238, mmurphy@gibsondunn.com)
[Abbey Hudson](#) – Los Angeles (+1 213.229.7954, ahudson@gibsondunn.com)

© 2024 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at gibsondunn.com.

Attorney Advertising: These materials were prepared for general informational purposes only based on information available at the time of publication and are not intended as, do not constitute, and should not be relied upon as, legal advice or a legal opinion on any specific facts or circumstances. Gibson Dunn (and its affiliates, attorneys, and employees) shall not have any liability in connection with any use of these materials. The sharing of these materials does not establish an attorney-client relationship with the recipient and should not be relied upon as an alternative for advice from qualified counsel. Please note that facts and circumstances may vary, and prior results do not guarantee a similar outcome.

SHAREHOLDER PROPOSAL DEVELOPMENTS DURING THE 2024 PROXY SEASON

To Our Clients and Friends:

This update provides an overview of shareholder proposals submitted to public companies during the 2024 proxy season,¹ including statistics and notable decisions from the staff (the “Staff”) of the Securities and Exchange Commission (the “SEC”) on no-action requests.²

I. SUMMARY OF TOP SHAREHOLDER PROPOSAL TAKEAWAYS FROM THE 2024 PROXY SEASON

As discussed in further detail below, based on the results of the 2024 proxy season, there are several key takeaways to consider for the coming year:

- ***Shareholder proposal submissions rose yet again.*** For the fourth year in a row, the number of proposals submitted increased. In 2024, the number of proposals increased by 4% to 929—the highest number of shareholder proposal submissions since 2015.
- ***The number of governance and social proposals increased, while civic engagement and environmental proposals decreased.*** Governance proposals increased notably, up 13% from 2023, with the increase largely attributable to proposals related to the adoption of prescriptive majority voting director resignation bylaws. The number of social proposals also increased, up 4% compared to 2023. In contrast, civic engagement and environmental proposals declined 10% and 4%, respectively. The five most popular proposal topics in 2024, representing 34% of all shareholder proposal submissions, were (i) climate change, (ii) nondiscrimination and diversity-related, (iii) simple majority vote, (iv) director resignation bylaws, and (v) independent chair. Of the five most popular topics in 2024, all but two were also in the top five in 2023 (simple majority vote and director resignation bylaws replaced shareholder approval of certain severance agreements and special meetings).

¹ Analyses of shareholder proposals and no-action letters often varies depending on the time period covered, data sources, and other factors. Please see footnote 3 for additional information on our methodology.

² Gibson, Dunn & Crutcher LLP assisted companies in submitting the shareholder proposal no-action requests discussed in this update that are marked with an asterisk (*).

- The no-action request volumes and outcomes appear to have reverted to pre-2022 norms, with the number of no-action requests increasing significantly and the percentage of proposals excluded pursuant to a no-action request continuing to rebound from 2022's historic low.*** There were 267 no-action requests submitted to the Staff in 2024, representing a submission rate of 29%, up significantly from a submission rate of 20% in 2023 and consistent with a submission rate of 29% in 2022. The overall success rate for no-action requests, after plummeting to only 38% in 2022, continued to rebound in 2024, with a success rate of 68%, compared to a success rate of 58% in 2023. Success rates in 2024 improved for resubmission, violation of law, ordinary business, and substantial implementation grounds, while success rates declined for procedural and duplicate proposal grounds.
- The number of proposals voted on increased yet again, but overall voting support remained at historically low levels, and only 4% of proposals submitted received majority support.*** In 2024, over 55% of all proposals submitted were voted on, compared with 54% of submitted proposals voted on in 2023. Average support across all shareholder proposals was 23.0%, roughly level with average support of 23.3% in 2023 and the lowest average support in over a decade. Average support for governance proposals increased from 2023, while overall support for both environmental and social proposals declined. In both cases, the decline appears to have been driven by the submission of proposals that are overly prescriptive or not particularly germane to a company's core operations and the low voting support for proposals that challenged companies' focus on certain ESG-related policies and practices. While the number of shareholder proposals that received majority support increased to 39 in 2024, up from 25 in 2023, majority-supported proposals still represented only 4% of proposals submitted, up slightly from 3% in 2023.
- Anti-ESG proposals proliferated in 2024, but shareholder support was low.*** The 2024 proxy season saw a continued rise in the use of the Rule 14a-8 process by proponents critical of corporate initiatives or corporate leadership that they view as inappropriately involved in environmental, social or political agenda (referred to as "anti-ESG" proposals). This year, 107 proposals were submitted by anti-ESG proponents, on topics ranging from traditional corporate governance matters to proposals challenging companies' diversity, equity and inclusion programs and opposing efforts to reduce greenhouse gas emissions. Of the proposals submitted by anti-ESG proponents, 78 were voted on, receiving average support of 2.4%. Notably, no anti-ESG proposal received more than 10% support.
- With SEC amendments to Rule 14a-8 and legislative reform efforts stalled, stakeholder challenges to the SEC's role in the shareholder proposal process foment uncertainty.*** In July 2022 the SEC proposed amendments to Rule 14a-8 to significantly narrow key substantive bases that companies use to exclude shareholder proposals on substantial implementation, duplication, and resubmission grounds remain stalled. At the same time, after a flurry of activity in July 2023, the Republican ESG Working Group formed by the Chair of the Financial Services Committee of the U.S. House of Representatives appears to have stalled in its

efforts to reform the Rule 14a-8 no-action request process. However, ongoing legal action by two stakeholder groups (the National Center for Public Policy Research (“NCPPr”) and the National Association of Manufacturers (“NAM”)), and Exxon Mobil Corp.’s legal challenge to a proposal, as well as recent Supreme Court decisions that could further invigorate challenges to the SEC’s authority to adopt Rule 14a-8, signal that uncertainty about the shareholder proposal process and the SEC staff’s role in adjudicating Rule 14a-8 no-action requests will persist.

- ***Proponents and third parties continue to use exempt solicitations to advance their agendas.*** Exempt solicitation filings remained at record levels, with the number of filings reaching a record high again this year—up over 69% compared to 2021. As in prior years, the vast majority of exempt solicitation filings in 2024 were filed by shareholder proponents on a voluntary basis—*i.e.*, outside of the intended scope of the SEC’s rules—in order to draw attention and publicity to pending shareholder proposals. Continuing a trend first noted last year, third parties are intervening in the shareholder proposal process by using exempt solicitation filings to provide their views on shareholder proposals submitted by unaffiliated shareholder proponents. In addition, some third parties have used exempt solicitation filings to disseminate their general views on social or governance topics beyond those raised by a specific shareholder proposal.

II. OVERVIEW OF SHAREHOLDER PROPOSAL OUTCOMES³

A. Overview of Shareholder Proposals Submitted

According to the available data, shareholders submitted 929 shareholder proposals during the 2024 proxy season, up 4% from 889 in 2023—marking the fourth consecutive year of increased submissions and the highest number of shareholder proposal submissions since 2015. The table below shows key year-over-year submission trends

³ **Data on No-Action Requests:** For purposes of reporting statistics regarding no-action requests, references to the 2024 proxy season refer to the period between October 1, 2023 and June 1, 2024. Data regarding no-action letter requests and responses was derived from the information available on the SEC’s website.

Data on Shareholder Proposals: Unless otherwise noted, all data on shareholder proposals submitted, withdrawn, and voted on (including proponent data) is derived from Institutional Shareholder Services (“ISS”) publications and the ISS shareholder proposals and voting analytics databases, with only limited additional research and supplementation from additional sources, and generally includes proposals submitted and reported in these databases for the calendar year from January 1 through June 1, 2024, for annual meetings of shareholders at Russell 3000 companies held on or before June 1, 2024. Consistent with last year, the data for proposals withdrawn and voted on includes information reported in these databases for annual meetings of shareholders held through June 1, 2024. References in this update to proposals “submitted” include shareholder proposals publicly disclosed or evidenced as having been delivered to a company, including those that have been voted on, excluded pursuant to a no-action request, or reported as having been withdrawn by the proponent, and do not include proposals that may have been delivered to a company and subsequently withdrawn without any public disclosure. All shareholder proposal data should be considered approximate. Voting results are reported on a votes-cast basis calculated under Rule 14a-8 (votes for or against) and without regard to whether the company’s voting standards take into account the impact of abstentions.

Where statistics are provided for 2023, the data is for a comparable period in 2023.

across five broad categories of shareholder proposals in 2024—governance, social, environmental, civic engagement, and executive compensation. As in 2023, social and environmental proposals combined represented over 50% of all proposals submitted (53% in 2024, down slightly from 55% in 2023), with social proposals representing 33% of all proposals submitted. This was followed by governance proposals (26%), environmental proposals (20%), civic engagement proposals (9%), executive compensation proposals (8%), and other proposals (4%). In reviewing these statistics, it should be noted that an increasing number of shareholder proposals could fall into more than one category. For example, proposals addressing political spending congruence or political contributions, as well as proposals addressing executive compensation, often serve as vehicles to raise social or environmental topics.⁴

⁴ Where a shareholder proposal addresses multiple topics, we have categorized the proposal based on the nature of the proposal's resolved clause, although the proposal's supporting statement or subsequently filed exempt soliciting materials may indicate a different focus. We categorize shareholder proposals based on subject matter as follows:

Governance proposals include proposals addressing: (i) independent board chair; (ii) shareholder special meeting rights; (iii) proxy access; (iv) majority voting for director elections; (v) board declassification; (vi) shareholder written consent; (vii) elimination/reduction of supermajority voting; (viii) director term limits; (ix) stock ownership guidelines; (x) shareholder approval of bylaw amendments; and (xi) director resignation bylaws.

Social proposals cover a wide range of issues and include proposals relating to: (i) discrimination and other diversity-related issues (including board diversity and racial equity audits); (ii) employment, employee compensation or workplace issues (including gender/ethnicity pay gap); (iii) board committees on social and environmental issues; (iv) social and environmental qualifications for director nominees; (v) disclosure of board matrices including director nominees' ideological perspectives; (vi) societal concerns, such as human rights, animal welfare, and reproductive health; (vii) employment or workplace policies, including the use of concealment clauses, mandatory arbitration, and other employment-related contractual obligations; and (viii) artificial intelligence.

Environmental proposals include proposals addressing: (i) climate change (including climate change reporting, climate lobbying, greenhouse gas emissions goals, and climate change risks); (ii) climate transition planning; (iii) plastics, recycling, or sustainable packaging; (iv) renewable energy; (v) environmental impact reports; and (vi) sustainability reporting.

Civic engagement proposals include proposals addressing: (i) political contributions disclosure; (ii) lobbying policies and practices disclosure; and (iii) charitable contributions disclosure.

Executive compensation proposals include proposals addressing: (i) severance and change of control payments; (ii) performance metrics, including the incorporation of sustainability-related goals; (iii) compensation clawback policies; (iv) equity award vesting; (v) executive compensation disclosure; (vi) limitations on executive compensation; and (vii) CEO compensation determinations.

Overview of Shareholder Proposals Submitted

Proposal Category	2024	2023	2024 vs 2023 ⁵	Observations
Social	308	297	↑4%	Social proposals addressed a wide range of topics in 2024, with the largest subcategory, nondiscrimination and diversity-related proposals, representing 15% of all social proposals, with 55 submitted in 2024 (down substantially from 76 in 2023 and 97 in 2022). Of note, the number of proposals related to reproductive healthcare fell from 22 in 2023 to 10 in 2024.
Governance	240	212	↑13%	Simple majority vote proposals were the most common governance proposal, representing 21% of these proposals with 51 submitted, up from 10 proposals in 2023. Proposals related to director resignation bylaws represented 19% of governance proposals with 46 submitted, up from six proposals in 2023.
Environmental	182	188	↓3%	The largest subcategory of environmental proposals, representing 71% of these proposals, continued to be climate change proposals, with 127 submitted in 2024 (down from 150 in 2023 and 129 in 2022). Of note, there were 11 climate change proposals submitted in 2024 that specifically addressed “just transition” issues related to worker impacts caused by a transition to a low-carbon economy.
Civic engagement	87	97	↓10%	The number of political spending congruence proposals fell to 13 from 21 in 2023. Lobbying spending proposals were roughly flat, with 35 in 2024 and 34 in 2023. Likewise, political contributions proposals were constant with 30 submissions in both 2024 and 2023.
Executive compensation	75	75	=	The largest subcategory of executive compensation proposals continued to be those requesting that boards seek shareholder approval of certain severance agreements, representing 44% of these proposals, down from 63% in 2023. Proposals implementing a binding bylaw amendment requiring shareholder approval of director compensation jumped to 13 in 2024 from zero in 2023, and proposals requesting

⁵ Data in this column refers to the percentage increase or decrease in shareholder proposals submitted in 2023 as compared to the number of such proposals submitted in 2022.

amendments to clawback policies for incentive compensation jumped to 12 in 2024, up from three in 2023. There were six proposals requesting that companies include, or report on the possibility of including, social- or environmental-focused performance measures in executive compensation programs (such as greenhouse gas (“GHG”) emissions and maternal morbidity) down from seven such proposals in 2023.

The table below shows that three of the five most common proposal topics during the 2024 proxy season were the same as those in the 2023 proxy season. Once again, the concentration of the top five most popular topics fell sharply from 45% of proposals submitted in 2023 to 34% of proposals submitted in 2024, demonstrating that proponents continue to submit proposals across a broad spectrum of topics. Proposals related to independent board chairs and nondiscrimination and diversity both fell sharply, collectively representing only 10% of proposals in 2024, down from 19% in 2023. A new proposal, requesting a director resignation bylaw, jumped into the top five, while shareholder approval of severance agreements dropped out of the top five.

Top Shareholder Proposals Submitted to Public Companies	
2024	2023
Climate change (14%)	Climate change (17%)
Nondiscrimination & diversity (6%)	Independent chair (10%)
Simple majority vote (5%)	Nondiscrimination & diversity (9%)
Director resignation bylaws (5%)	Shareholder approval of severance agreements (5%)
Independent chair (5%)	Special meeting (5%)

B. Overview of Shareholder Proposal Outcomes

As shown in the table below, the 2024 proxy season saw both new and continued trends in proposal outcomes that emerged in the 2023 proxy season: (i) the percentage of proposals voted on increased only slightly (55% in 2024 compared to 54% in 2023), and overall support was roughly level (23.0% in 2024 compared to 23.3% in 2023); (ii) the percentage of proposals excluded through a no-action request increased substantially (15% in 2024 compared to 9% in 2023); and (iii) the percentage of proposals withdrawn decreased slightly (15% in 2024 compared to 16% in 2023).

Social and environmental proposals both saw lower withdrawal rates for the second year in a row, with 12% of social proposals withdrawn in 2024 (compared to 20% in 2023 and 30% in 2022) and 29% of environmental proposals withdrawn in 2024 (compared to 32% in 2023 and 51% in 2022). Shareholder proponents may still be relying on the perception that Staff Legal Bulletin No. 14L (Nov. 3, 2021) (“SLB 14L”) signaled increased Staff skepticism of Rule 14a-8 no-action requests, therefore making proponents less willing to withdraw their proposals. However, as discussed below and

perhaps as a result of increasingly prescriptive shareholder proposals, the number of no-action requests granted reverted to the pre-SLB 14L norm in 2024, with the Staff granting approximately 68% of no-action requests. This represents a marked increase over the 58% success rate in 2023, a significant increase over the 38% success rate in 2022, and edges closer to the 71% success rate in 2021.

The percentage of withdrawn governance proposals increased to 12%, three times the 2023 withdrawal rate of 4%, and above both its 2022 and 2021 rates of 9% and 5%, respectively. Director resignation bylaw proposals made up a significant portion of withdrawn governance proposals, likely as a result of the Staff's concurrence with no-action requests arguing that implementation of the proposals would cause the companies to violate Delaware law.

Shareholder Proposal Outcomes⁶		
	2024	2023
Total number of proposals submitted	929	889
Excluded pursuant to a no-action request	15% (141)	9% (82)
Withdrawn by the proponent	15% (135)	16% (143)
Voted on	55% (514)	54% (483)

Voting results. Shareholder proposals voted on during the 2024 proxy season averaged support of 23.0%, roughly level with average support of 23.3% in 2023. Notably, average support was depressed in part due to the voting results for anti-ESG proposals, which received average support of just 2.4%. Excluding the 78 anti-ESG proposals that were voted on, average support was 26.8%. Looking at voting results across the environmental, social and governance categories:

- **Environmental proposals.** Average support decreased for the second year in a row to 18.7%, down from 21.3% in 2023 and 33.3% in 2022. That decreased support was driven primarily by the voting results for the 13 prescriptive anti-ESG proposals that were voted on in 2024, which averaged less than 2% support. Removing these proposals results in average support for environmental proposals of 21.7%. Consistent with the trend we saw in 2023 and 2022 and as discussed below, the continued lower support for climate change proposals appears to be driven by an increase in more prescriptive or non-germane proposals, which have received lower support from institutional investors.
- **Social proposals.** Average support decreased to 13.5% in 2024 down from 17.2% in 2023 and 23.2% in 2022. This decrease appears to be largely driven by the voting results on the 43 social proposals submitted by anti-ESG

⁶ Statistics on proposal outcomes exclude proposals that were reported in the ISS database as having been submitted but that were not in the proxy or were not voted on for other reasons, including, for example, due to a proposal being withdrawn but not publicized as such or the failure of the proponent to present the proposal at the meeting. Outcomes also exclude proposals that were to be voted on after June 1. As a result, in each year, percentages may not add up to 100%. ISS reported that 91 proposals (representing 10% of the proposals submitted during the 2024 proxy season) remained pending as of June 1, 2024, and 118 proposals (representing 13% of the proposals submitted during the 2023 proxy season) remained pending as of June 1, 2023.

proponents that were voted on, which garnered average support of less than 2%. Excluding proposals submitted by these proponents, average support for social proposals was 17.4% on 134 voted proposals.

- **Governance proposals.** As in prior years, corporate governance proposals received generally high levels of support. Average support for governance proposals increased to 42% from 31% in 2023.

Of particular note, despite roughly level average support for proposals year-over-year, the percentage of proposals across all topics voted on in 2024 that received less than 5% support, the lowest resubmission threshold under Rule 14a-8(i)(12), increased markedly from 2023. In 2024, 100 of the 514 proposals voted on during the 2024 proxy season (almost 20%) received less than 5% support, compared with 62 proposals (12%) that received less than 5% support in 2023.

The table below shows the five shareholder proposal topics voted on at least three times that received the highest average support in 2024. Three of the top five shareholder proposals by average shareholder support in 2024 were different from those reported in 2023.⁷

Top Five Shareholder Proposals by Voting Results⁸		
Proposal	2024	2023
Simple majority vote (eliminate supermajority voting)	70.4% (38)	57.9% (16)
Declassify board of directors	54.3% (3)	N/A
Shareholder special meeting rights	43.4% (22)	31.3% (35)
Shareholder right to act by written consent	37.9% (7)	32.7% (6)
Repeal any bylaw provision adopted by the board without shareholder approval	34.1% (3)	N/A

Majority-supported proposals. As of June 1, 2024, 39 proposals (4% of the proposals submitted and 8% of the proposals voted on) received majority support, as compared with 25 proposals (or less than 3% of the proposals submitted and 5% of the proposals voted on) that had received majority support as of June 1, 2023. As in 2023, after several consecutive years of growth in the number of majority-supported climate change proposals, only two climate change proposals received majority support in 2024. These proposals were both submitted by The Accountability Board to Jack in the Box Inc. and Wingstop Inc. requesting disclosure of GHG reduction targets. Of the remaining 37 proposals that received majority support, 36 were corporate governance-related (27 of which requested simple majority votes), and one requested a report on

⁷ In 2023, the five shareholder proposals voted on at least three times that received the highest average support were simple majority vote (eliminate supermajority voting), reporting on climate lobbying, third-party assessments of companies' commitment to freedom of association, majority voting for director elections, and workplace health and safety audits. No proposals seeking to declassify the board of directors or repeal bylaw provisions adopted by the board without shareholder approval were voted on in 2023.

⁸ The numbers in the parentheses indicate the number of times these proposals were voted on.

political contributions. ISS recommended votes “for” all proposals that received majority support.

Notably, the 39 majority-supported proposals related to only eight different topics. While governance proposals have consistently ranked among the highest number of majority-supported proposals, in 2024 they accounted for 92% of these proposals (up significantly from 64% in 2023). No social or executive compensation proposals received majority support in 2024, a significant change from 2023 when environmental and social proposals together represented 24% of majority-supported proposals, while 8% related to executive compensation. None of these proposals were related to human capital management, diversity, equity and inclusion (“DEI”), collective bargaining, or workplace harassment and discrimination. The table below shows the proposals that received majority support.

Proposals that Received Majority Support

Proposal	2024	2023 ⁹
Simple majority vote (eliminate supermajority voting)	27	8
Shareholder special meeting rights	4	5
Climate change	2	2
Declassify board of directors	2	0
Adopt proxy access right	1	0
Report on political contributions	1	0
Repeal any bylaw provision adopted by the board without shareholder approval	1	0
Submit poison pill to shareholder vote	1	0

III. SHAREHOLDER PROPOSAL NO-ACTION REQUESTS

A. Overview of No-Action Requests

Submission and withdrawal rates. The number of shareholder proposals challenged in no-action requests during the 2024 proxy season increased significantly, up 53% compared to 2023 and up 9% compared to 2022. The submission rate was up significantly from 2023 and consistent with the submission rate in 2022. Gibson Dunn remains a market leader for handling shareholder proposals and related no-action requests, having filed approximately 20-25% of all shareholder proposal no-action requests each proxy season for several years.

⁹ Indicates the number of similar proposals that received majority support in 2023.

No-Action Request Statistics

	2024	2023	2022
No-action requests submitted	267	175	244
Submission rate ¹⁰	29%	20%	29%
No-action requests withdrawn	57 (21%)	33 (19%)	56 (23%)
Pending no-action requests (as of June 1)	3	0	3
Staff Responses ¹¹	207	142	185
Exclusions granted	141 (68%)	82 (58%)	71 (38%)
Exclusions denied	66 (32%)	60 (42%)	114 (62%)

Most common arguments. The table below, reflecting the number of no-action requests that contained each type of argument, shows a change in the most-argued grounds for exclusion from procedural in 2023 to ordinary business in 2024. As in recent years, ordinary business and substantial implementation continued to be the most argued substantive grounds for exclusion.

Most Common Arguments for Exclusion

	2024	2023	2022
Ordinary Business	105 (39%)	68 (39%)	106 (43%)
Procedural	88 (33%)	71 (41%)	64 (26%)
Substantial Implementation	59 (22%)	38 (22%)	91 (37%)
False/Misleading	44 (16%)	17 (10%)	42 (17%)

Success rates. This year, the Staff granted approximately 68% of no-action requests, a significant increase over the 58% success rate in 2023 and the 38% success rate in 2022, and edging closer to the 71% success rate in 2021 and the 70% success rate in 2020. The Staff most often granted no-action requests based on ordinary business (representing 40% of successful requests), procedural (representing 29% of successful requests), and violation of law (representing 16% of successful requests) grounds. However, it remains to be seen whether this was a one-year phenomena due to two new widely submitted proposals that were excluded on the grounds that the proposals would cause companies to violate state law. Notably, 85% of successful no-action requests in 2024 were based on one of these three grounds, reflecting a narrowing concentration of the grounds on which successful requests were granted in recent years.

¹⁰ Submission rates are calculated by dividing the number of no-action requests submitted to the Staff by the total number of proposals reported to have been submitted to companies.

¹¹ Percentages of exclusions granted and denied are calculated by dividing the number of exclusions granted and the number denied, each by the number of Staff responses.

Success Rates by Exclusion Ground¹²

	2024	2023	2022
Resubmission	88%	43%	56%
Violation of law	79%	33%	40%
Procedural	68%	80%	68%
Ordinary business	67%	50%	26%
Duplicate proposals	50%	100%	31%
Substantial implementation	33%	26%	15%

Top proposals challenged. This year, the most common proposals for which companies submitted no-action requests (on both procedural and substantive grounds) were those requesting adoption of director resignation bylaws, reporting of registered holder share totals in quarterly and annual reports, simple majority vote (elimination of supermajority voting provisions), and a policy requiring an independent board chair.

The no-action requests related to director resignation bylaws proposals made the following arguments: violation of law (20), lack of authority (12), procedural (9), violation of proxy rules (2), improper subject under state law (1), director election, (1), and substantial implementation (1). Fourteen successful requests were granted on violation of law grounds, and the five remaining were granted on procedural grounds.

The no-action requests related to registered holder share total reporting proposals made the following arguments: procedural (15), ordinary business (2), violation of proxy rules (2), and substantial implementation (1). All seven successful requests were granted on procedural grounds.

The no-action requests related to simple majority vote proposals made the following arguments: substantial implementation (7), procedural (4), violation of proxy rules (2), and lack of authority (1). Four successful requests were granted on substantial implementation grounds, and the three remaining successful requests were granted on procedural grounds.

The no-action requests related to independent board chair proposals made the following arguments: duplicate proposal (3), resubmission (3), procedural (1), and director election (1). The successful requests were granted on the following grounds: resubmission (2), duplicate proposal (2), procedural (1), and director election (1).

Top Proposals Challenged

	Submitted	Denied	Granted	Withdrawn
Director resignation bylaws	29	2 (7%)	19 (65%)	8 (28%)
Registered holder share total report	15	N/A	7 (47%)	8 (53%)
Simple majority vote	12	5 (42%)	7 (58%)	N/A
Independent board chair	8	N/A	6 (75%)	2 (25%)

¹² Success rates are calculated by dividing the number of no-action requests granted on a particular ground by the total number of no-action requests granted or denied on that ground, excluding no-action requests that are withdrawn or granted on an alternative ground.

B. Key No-Action Request Developments

There were a number of noteworthy procedural and substantive developments in no-action decisions this year.

1. Success Rates Edge Closer to Pre-SLB 14L Averages

During the last three proxy seasons, companies have confronted steady increases in the number of shareholder proposals submitted and at the same time appeared to be reconsidering the extent to which they pursued the no-action request process. After submitting 272 no-action requests to the Staff in the 2021 proxy season, companies submitted only 175 no-action requests in the 2023 proxy season, with the sharp decline likely spurred by significantly lower success rates during 2022, which saw the Staff grant relief to only 38% of no-action requests (down from success rates of 71% and 70% in 2021 and 2020, respectively). Success rates in 2022 declined on every basis for exclusion, with the most drastic decline in procedural, substantial implementation, and ordinary business arguments. The lower success rates were driven by the Staff's issuance of SLB 14L, which rescinded certain Staff guidance and reversed long-standing no-action decisions by abandoning the economic nexus standard, upending the Staff's recent approach to economic relevance under Rule 14a-8(i)(5) and the ordinary business exclusion under Rule 14a-8(i)(7). However, while the number of no-action requests submitted in 2023 dropped significantly, the percentage of proposals excluded pursuant to a no-action request rebounded from the historic low in 2022. The overall success rate for no-action requests rose to 58% in 2023—still well below recent success rates and the second-lowest success rate since 2012.

The 2024 proxy season saw a continued rebound in the success rates of no-action requests, with the Staff granting relief to approximately 68% of no-action requests. Unlike the rise in success rates in 2023 (which could be attributed in part to the sharp decline in overall no-action requests submitted), the 2024 proxy season saw a continued rise in success rates even as submission rates increased with companies returning to the no-action request process following the significant improvement in success rates seen in 2023. Success rates in 2024 improved for ordinary business (67%, up from 50% in 2023), resubmission (88%, up from 43% in 2023), violation of law (79%, up from 33% in 2023) and substantial implementation grounds (33%, up from 26% in 2023), while success rates declined for procedural (68%, down from 80% in 2023) and duplicate proposals (50%, down from 100% in 2023).

2. Spotlight on Micromanagement and Greenhouse Gas Emissions Proposals

After cratering in 2022 in the wake of SLB 14L, the submission rate and success rate for micromanagement no-action requests continued to recover in 2024: companies argued micromanagement in 62 no-action requests in 2024, up from 41 in 2023. To date, the Staff has granted 23 of those requests on that basis, representing a success rate of 66%, more than double the 2023 success rate of 31%. The marked rise in the success rate of micromanagement arguments is at least partially attributable to proponents

continuing to draft very prescriptive proposals. Proposals that the Staff concurred improperly micromanaged included those related to greenhouse gas (“GHG”) emissions and climate change,¹³ disclosure of director political and charitable contributions,¹⁴ disclosure of director time commitments,¹⁵ reports on living wage policies and practices,¹⁶ corporate charitable contributions,¹⁷ anti-union expenditures¹⁸ and the benefits and drawbacks of permanently committing not to sell paint products containing titanium dioxide sourced from the Okefenokee Swamp.¹⁹

The resurgence in successful micromanagement arguments is perhaps most clearly demonstrated in the number of climate change-related proposals that were successfully excluded in 2024. Of the 15 no-action requests challenging climate change-related proposals on substantive grounds, 12 argued for exclusion on the basis of micromanagement, with the Staff granting 10 of those requests on that basis²⁰ and denying only one request,²¹ with one request being withdrawn.²² Notably, each of the successful no-action requests challenged a proposal focused on the reduction of GHG emissions, including proposals requesting reports on GHG emissions of company clients, GHG emissions related to specific goods and services, the adoption of specific GHG emissions reduction targets, and reports on the divestiture of assets with “material climate impact.”

As the legal challenges to the SEC’s final climate disclosure rules continue to work their way through the U.S. Court of Appeals for the Eighth Circuit, climate change shareholder proposals (particularly those focused on GHG emissions) will undoubtedly remain a focus for shareholder proponents and companies, alike. The results in 2024 suggest that the no-action request process will continue to provide companies with a key means of challenging overly prescriptive climate change proposals, including those tied to GHG emissions.

¹³ See, e.g., *Wells Fargo & Co.* (avail. Mar. 6, 2024, *recon. denied* Apr. 5, 2024)*; *Chevron Corp.* (avail. Mar. 29, 2024)*; *Tractor Supply Co.* (avail. Mar. 18, 2024).

¹⁴ *Comcast Corp.* (avail. Apr. 16, 2024)*.

¹⁵ See, e.g., *Lowe’s Companies, Inc.* (avail. Apr. 8, 2024)*; *Johnson & Johnson* (avail. Mar. 1, 2024).

¹⁶ See, e.g., *Amazon.com, Inc.* (avail. Apr. 1, 2024)*; *Kohl’s Corp.* (avail. Mar. 6, 2024).

¹⁷ *Paramount Global* (avail. Apr. 19, 2024).

¹⁸ *Delta Airlines, Inc.* (avail. Apr. 24, 2024).

¹⁹ See, e.g., *Home Depot, Inc.* (avail. Mar. 21, 2024)*; *Chemours Co.* (avail. Feb. 22, 2024).

²⁰ See, e.g., *Walmart Inc.* (avail. Apr. 18, 2024)*; *Bank of America Corp.* (avail. Feb. 29, 2024, *recon. denied* Apr. 15, 2024)*; *The Goldman Sachs Group, Inc.* (avail. Mar. 4, 2024, *recon. denied* Apr. 15, 2024)*; *Wells Fargo & Co.* (avail. Mar. 6, 2024, *recon. denied* Apr. 5, 2024)*; *Morgan Stanley* (avail. Mar. 29, 2024); *Chevron Corp.* (avail. Mar. 29, 2024)*; *JPMorgan Chase & Co.* (avail. Mar. 29, 2024); *Valero Energy Corp.* (avail. Mar. 22, 2024); *Exxon Mobil Corp.* (avail. Mar. 20, 2024); *Tractor Supply Co.* (avail. Mar. 18, 2024).

²¹ *Chubb Ltd.* (avail. Mar. 25, 2024).

²² *The TJX Companies, Inc.* (avail. Apr. 12, 2024)*.

3. Violation of Law Arguments – Director Resignation and Director Compensation Bylaw Proposals

The 2024 proxy season saw a marked increase in both the submission and success of no-action requests seeking exclusion on violation of law grounds. This increase was driven primarily by a shareholder proposal campaign spearheaded by pension funds affiliated with the United Brotherhood of Carpenters and Joiners of America (the “Carpenters”). The proposal asked companies to amend their bylaws to require that directors tender an irrevocable resignation to the company, effective upon the director’s failure to receive majority support in an uncontested election, and that the board accept

the resignation offer unless it finds a “compelling reason or reasons” not to accept the resignation.

Of the 29 no-action requests submitted challenging the Carpenters’ proposals under Rule 14a-8(i)(2), 14 were granted on the grounds that the proposal would cause the company to violate state law,²³ five were granted on separate procedural grounds, and eight were withdrawn. Only two no-action requests were denied on violation of law grounds.²⁴ Notably, both of those requests were submitted to companies incorporated outside of Delaware and did not include a separate opinion letter from local counsel explaining how the proposal would cause the company to violate state law.

In addition to the director resignation bylaw proposals, a number of companies also challenged under Rule 14a-8(i)(2) proposals seeking to implement binding bylaw amendments imposing specific limitations and requirements on how director compensation is fixed. In all eight no-action requests, the companies included a separate opinion letter from local counsel.²⁵ As of June 1, the Staff had issued responses to six of the no-action requests—in each case, granting the request on violation of law grounds and citing the state law legal opinion submitted in support of the no-action request.

In light of the results in violation of law arguments during 2024, companies should strongly consider providing a separate opinion letter from local counsel in support of the no-action request consistent with prior Staff guidance.²⁶

²³ See, e.g., *MetLife, Inc.* (avail. Apr. 22, 2024); *Gartner, Inc.* (avail. Mar. 29, 2024)*; *AT&T Inc.* (avail. Mar. 19, 2024)*; *Verizon Communications, Inc.* (avail. Apr. 15, 2024).

²⁴ *Xerox Holdings Corp.* (avail. Apr. 8, 2024) (incorporated in Connecticut); *Altria Group, Inc.* (avail. Mar. 25, 2024) (incorporated in Virginia).

²⁵ See, e.g., *General Motors Co.* (avail. Apr. 18, 2024); *VeriSign, Inc.* (avail. Mar. 29, 2024)*.

²⁶ See Staff Legal Bulletin No. 14B (Sep. 15, 2004) (noting that consistent with Rule 14a-8(j)(2)(iii), which requires a supporting opinion of counsel when the asserted reasons for exclusion are based on matters of state or foreign law, no-action requests arguing for exclusion under Rule 14a-8(i)(2) and/or Rule 14a-8(i)(6) should be accompanied with a supporting opinion of counsel).

4. Substantial Implementation Holding on by a Thread

As discussed above, while the success rate for no-action requests seeking exclusion on substantial implementation grounds increased in 2024, it remained well below the success rate in 2021. In fact, the Staff granted only nine no-action requests in 2024 on the basis of substantial implementation, representing only 6% of no-action requests granted. While the low number of successful substantial implementation requests was due in part to the withdrawal of 16 no-action requests arguing that basis, most of which involved a proposal regarding advance notice bylaws submitted by James McRitchie, it is important to note that the Staff rejected 18 no-action requests that argued substantial implementation—double the number of no-action requests it granted on that basis.

Substantial implementation arguments were most successful in the context of corporate governance and executive compensation proposals, including proposals related to declassification of the board,²⁷ the adoption of simple majority vote,²⁸ clawback policy amendments,²⁹ and shareholder approval of executive severance packages.³⁰ Notably, no social or environmental proposals were successfully excluded on substantial implementation grounds in 2024—broadly consistent with results in 2023, when only one environmental proposal and no social proposals were excluded on that basis.

5. Successful Exclusion of Resubmissions on the Rise

In recent years, an increasing percentage of shareholder proposals have been submitted and voted on annually, while at the same time, overall support for shareholder proposals has continued to decrease year-over-year as shareholders are faced with increasingly prescriptive proposals disfavored by institutional investors. In addition, some institutional investors have noted that at the same time there has been a decrease in the overall quality and accuracy of shareholder proposals, and an increase in the submission of proposals that are not well targeted to a specific company and that address topics unrelated to a company's core activities.³¹

Despite these overall trends, some shareholder proponents have continued to repeatedly resubmit unsuccessful proposals. Due in part to continued declines in shareholder support, the 2024 proxy season saw a marked increase in the number of proposals successfully excluded under the resubmission thresholds in Rule 14a-8(i)(12). Rule 14a-8(i)(12) permits exclusion of a proposal if a similar proposal was included in the proxy materials within the preceding three years, and if the last time a similar proposal was included it received: less than 5% support, if voted on once within the last five years; less than 15% support, if voted on twice within the last five years; or less than 25% support, if voted on three or more times within the last five years.

²⁷ *Kyndryl Holdings, Inc.* (avail. Apr. 22, 2024).

²⁸ *PulteGroup, Inc.* (avail. Mar. 19, 2024); *Eli Lilly and Co.* (avail. Mar. 14, 2024); *West Pharmaceutical Services, Inc.* (avail. Mar. 13, 2024); *AECOM* (avail. Jan. 4, 2024).

²⁹ *Amgen Inc.* (avail. Apr. 3, 2024); *Exxon Mobil Corp.* (avail. Mar. 20, 2024).

³⁰ *Expeditors International of Washington, Inc.* (avail. Mar. 15, 2024).

³¹ See, for example, T. Rowe Price, *For or against? The year in shareholder resolutions—2023* (April 2024), available [here](#).

In 2024, seven proposals were successfully excluded under Rule 14a-8(i)(12) for failure to receive a sufficient level of support,³² more than double the three successful no-action requests in 2023 and representing a success rate of 88%. An additional six proposals arguing for exclusion on that basis were withdrawn before the Staff could issue its decision. The proposals challenged by the successful no-action requests addressed a wide range of topics, including reports on lobbying activities, independent board chairs, majority voting in uncontested director elections, GHG emissions reductions, and workplace civil liberties.

IV. KEY SHAREHOLDER PROPOSAL TOPICS DURING THE 2023 PROXY SEASON

A. Human Capital and Social Proposals

This year saw a marked decline in proposals focused on nondiscrimination and diversity. These proposals accounted for only about 18% of social proposals in 2024, after constituting over one-quarter of social proposals in 2023. Like last year, human capital and social proposals were largely focused on racial equity and civil rights, DEI efforts, and pay equity. There was also a significant decline in proposals focused on reproductive rights this year, while there were slightly more proposals related to human rights assessments. The 2024 proxy season also continued to see a significant rise in social proposals directly challenging traditional ESG themes. These anti-ESG social proposals included proposals requesting that companies, among other things, report on risks created by diversity, equity and inclusion efforts, conduct a civil rights and nondiscrimination audit, report on risks related to discrimination based on religious or political views, and report on gender-based compensation and benefits inequities related to transgender healthcare.

1. Racial Equity/Civil Rights Audit and Nondiscrimination Proposals

In 2024, there were 22 shareholder proposals that addressed issues of racial equity and civil rights (including workplace discrimination, audits of workplace practices and policies, and related topics), compared to 55 similar proposals submitted in 2023 and 51 in 2022.

The most frequent type of these proposals were the 13 proposals calling for a racial equity or civil rights audit analyzing each company's impacts on the "civil rights of company stakeholders" or "civil rights, diversity, equity, and inclusion." Similar to prior years, these proposals often included the required or optional use of a third party to conduct the audit, with input to be solicited from employees, customers, civil rights organizations, and other stakeholders. These proposals were primarily submitted by the Service Employees International Union and the Nathan Cummings Foundation. Five of these proposals went to a vote and received average support of 12.9%, down from 14 such proposals that went to a vote in 2023, with average support of 22.4%. In both years, ISS generally recommended votes "against" the proposals. Two companies initially filed no-action requests to exclude a racial equity/civil rights audit proposal on

³² Kroger Co. (avail. May 3, 2024); AMC Networks, Inc. (avail. Apr. 22, 2024); Exxon Mobil Corp. (avail. Mar. 20, 2024); The Coca-Cola Co. (avail. Feb. 22, 2024); Baxter International Inc. (avail. Feb. 20, 2024); Applied Materials, Inc. (avail. Jan. 4, 2024); Ingles Markets, Inc. (avail. Nov. 6, 2023).

substantial implementation and procedural grounds but later withdrew the challenges after the proposals were withdrawn.³³

In addition, in 2024 there were nine proposals related to workplace nondiscrimination, including requests to report on harassment and discrimination statistics, efforts to prevent workplace harassment and discrimination, and hiring practices related to formerly incarcerated people. These proposals were vastly outnumbered by 22 anti-ESG proposals related to viewpoint discrimination, calling for a civil rights and nondiscrimination audit, or expressing concern about discrimination on the basis of religious or political views, submitted by organizations such as the NCPPR, The Bahnsen Family Trust, Inspire Investing LLC, and the American Family Association. These proposals generally included supporting statements that focused on concerns about discrimination against “non-diverse” employees or discrimination based on religious and political views.

No companies sought to exclude workplace nondiscrimination proposals on substantive grounds. However, one company unsuccessfully sought to exclude an anti-ESG nondiscrimination proposal on substantive grounds, which was ultimately unsuccessful.³⁴ The eight nondiscrimination proposals that went to a vote (excluding anti-ESG nondiscrimination proposals) averaged 14.8% support, as compared to average support of 1.9% support for anti-ESG nondiscrimination proposals that went to a vote.

2. Diversity, Equity, and Inclusion Efforts and Metrics

The number of proposals requesting disclosure of DEI data or metrics or reporting on the effectiveness of DEI efforts or programs decreased slightly, with 28 such proposals submitted in 2024 compared to 35 in 2023. Of the 2024 DEI proposals, 14 proposals were withdrawn or otherwise not included in the proxy statement and 10 were voted on with an average support of 25.0%. No proposals received majority support. Four companies filed no-action requests to exclude DEI proposals on procedural grounds, two of which were withdrawn and two of which were successful. As in 2023 and 2022, As You Sow was the main driver behind these proposals, submitting or co-filing 17 DEI proposals. Other filers included the New York State Comptroller on behalf of the New York State Common Retirement Fund (submitting three proposals), Trillium Asset Management (submitting three proposals) and Amalgamated Bank (submitting three proposals co-filed by As You Sow).

3. Gender/Racial Pay Gap

The number of shareholder proposals calling for a report on the size of a company’s gender and racial pay gap and policies and goals to reduce that gap remained relatively flat, with 15 proposals submitted in 2024 versus 16 in 2023. Eight gender/racial pay gap proposals were submitted or co-filed by Arjuna Capital and five were submitted by James McRitchie and/or Myra Young. Fourteen of these proposals were voted on,

³³ *Valero Energy Corp.* (avail Feb. 2, 2024); *Equifax, Inc.* (avail. Jan. 12, 2024).

³⁴ *AT&T Inc.* (avail. Feb. 29, 2024)*.

garnering average support of 29.2% (with none receiving majority support). This represented a modest decrease from average support of 31.7% for the nine proposals voted on in 2023 (with none receiving majority support).

4. Reproductive Rights

In the second proxy season since the overturn of *Roe v. Wade*, the number of shareholder proposals requesting a report on the effect of reproductive healthcare legislation decreased significantly, with only 10 such proposals submitted in 2024, including two proposals submitted by anti-ESG proponents, down from 22 proposals in 2023. Six of these proposals were voted on, averaging 6.5% support, including the two anti-ESG proposals that averaged 1.3% support, a decrease from average support of 10.8% in 2023.

5. Human Rights

The number of shareholder proposals relating to human rights, including those calling for a report on or an impact assessment of risks of doing business in countries with significant human rights concerns or for an assessment of the human rights impacts of certain products or operations, decreased during the 2024 proxy season. In 2024, shareholders submitted 39 human rights proposals (down from 43 proposals in 2023). Eight proposals were submitted by anti-ESG proponents requesting reports on the risk of the company's operations in China and the congruency of human rights policies with company actions. The 28 human rights proposals voted on averaged support of 12.4%, with the proposals submitted by anti-ESG proponents averaging support of 2.9% and the remainder averaging support of 16.2%. Six companies sought to exclude these proposals via no-action requests, and two were successful on the grounds that the proposals related to ordinary business operations.³⁵

6. Animal Welfare

There were 24 shareholder proposal submissions related to animal welfare in 2024, a notable increase from 14 in 2023. These proposals most commonly requested disclosures related to pig gestation crates or egg-laying hens. Fourteen of these proposals went to a vote, receiving average support of 16.4%. None of these proposals received majority support. Only one proposal was challenged with the SEC, but the challenge was ultimately withdrawn. All but one of the proposals were either filed or co-filed by The Humane Society of the United States, The Accountability Board, or the People for the Ethical Treatment of Animals (PETA).

³⁵ *AT&T Inc.* (avail. Mar. 14, 2024)*; *Verizon Communications Inc.* (avail. Mar. 14, 2024).

B. AI Proposals

Issues related to the development and use of artificial intelligence (AI) were a growing focus for shareholder proposals in 2024. Fourteen AI proposals were submitted during 2024,³⁶ covering a variety of topics related to AI. Among the proposals submitted were proposals calling for a report on a company's current or future use of AI, requesting a report on risks from misinformation and disinformation related to AI, and requesting the board formalize oversight of AI. The SEC appeared to treat any proposal addressing AI as involving a significant policy issue, likely reflecting Chair Gensler's focus on the topic. ISS recommended votes "for" five proposals requesting AI-related reports. However, ISS recommended votes "against" two proposals requesting that the company take action to formalize board oversight of AI matters—one proposal requested the board create an AI committee, and the other proposal requested changes to the company's audit and compliance committee charter to address AI oversight. Despite ISS's general support for AI proposals, all ultimately failed to receive majority support. As of June 30, 2024, 10 such proposals had been voted on, receiving average support of 20.9%.³⁷ The Staff denied all three no-action requests challenging AI proposals on ordinary business and/or micromanagement grounds.

C. Continued Focus on Climate Change and Environmental Proposals

As was the case in 2023, climate change-related proposals were the largest group of environmental shareholder proposals in 2024 by a large margin, representing 70% of all environmental proposals (and 14% of all proposals) submitted. There were 127 climate change-related proposals submitted in 2024, down from 150 proposals in 2023. There also was an increase in the number of environmental and climate change proposals excluded during 2024 via no-action requests, with 19 excluded (three on procedural grounds,³⁸ one on resubmission grounds,³⁹ and the rest on ordinary business or micromanagement grounds), as compared to 13 excluded during 2023 (five on procedural grounds, one on substantial implementation grounds, and seven on ordinary business or micromanagement grounds). These exclusions were consistent with the overall rise in the success of ordinary business arguments more generally (as described in Part III above).

Climate change proposals took various forms, including requesting adoption of GHG emissions reduction targets (usually in alignment with net zero scenarios), disclosure of climate transition plans, disclosures regarding single-use plastics, changes to investments in and underwriting policies relating to fossil fuel production projects, and

³⁶ One additional AI proposal was submitted to a company with an annual meeting in December 2023 but is not included in the 14 proposals above because the submission occurred outside of the 2024 proxy season. Like the AI proposals voted on during the 2024 proxy season, this 2023 AI proposal also failed, receiving 21.2% support.

³⁷ Due to the number of AI proposals that were voted on after June 1, 2024, we have included the voting results for several proposals voted on at annual meetings on or before June 30, 2024.

³⁸ *Linde plc* (avail. Apr. 24, 2024); *Amazon.com, Inc.* (avail. Apr. 5, 2024)*; *Bank of America Corp.* (avail. Feb. 20, 2024)*.

³⁹ *Exxon Mobil Corp.* (avail. Mar. 20, 2024).

disclosures of risks related to climate change. Of these, the most common were proposals focusing on GHG disclosures (and, in particular, the scope of emissions covered by such disclosures), emissions reductions targets, and climate transition plans. Other popular climate change proposals included requests that companies disclose their Clean Energy Supply Financing Ratio and assess their biodiversity impacts. As with social proposals, there was also a rise in climate change proposals from anti-ESG activists, including proposals calling for a board committee to analyze the risks of committing to decarbonization.

Continuing the trend from 2023, average support for these proposals and the number receiving majority support are all equal to or at their lowest rates in at least three years. However, ISS support for climate change proposals increased in 2024, with ISS recommending votes “for” 56% of climate change proposals, up from 47% in 2023. Excluding anti-ESG climate change proposals, ISS recommended votes “for” 69% of climate change proposals. Two climate change proposals received majority support in 2024. Both proposals were submitted by The Accountability Board and requested that the company disclose its GHG emissions, as well as short-, medium- and long-term goals for reducing those emissions.

Climate Change Proposal Statistics: 2024 vs. 2023			
	2024	2023	2024 vs. 2023
Submitted	127	150	↓15%
Voted on	68	70	↓3%
Average support	20.2%	22.0%	↓8%
Majority support	2	2	-
Withdrawn (as percentage of submitted)	24%	30%	↓20%

1. Climate Transition Plans

There were 51 shareholder proposals requesting a climate transition report, including proposals requesting disclosure of the company’s GHG emissions reduction targets as well as policies, strategies, and progress made toward achieving those targets. These proposals usually called for long-term GHG emissions targets covering Scopes 1, 2, and 3 emissions and in alignment with the Paris Agreement’s 1.5 degree Celsius net zero scenario and the Science Based Targets initiative (SBTi), including by asking companies to expand established emissions targets that do not meet these requirements. These proposals’ supporting statements frequently referenced concerns that disclosure of emissions reduction targets is not enough to address climate risk or provide sufficient accountability for achieving those targets and that investors would benefit from increased disclosure regarding the company’s strategies to achieve those targets, including relevant timelines and metrics against which to measure progress. In a dramatic increase from last year, 12 proposals in 2024 (versus four in 2023) asked financial institutions to adopt transition plans to align the company’s financing activities with its GHG emissions reduction targets. There was also a notable increase (11 proposals in 2024 versus five in 2023) in proposals focused on the impact of a company’s climate transition strategy on relevant stakeholders under the International Labour Organization’s “just transition” guidelines. The primary proponents of climate

transition proposals were As You Sow (submitting or co-filing 12 proposals), Green Century Capital Management (submitting or co-filing eight proposals), and Arjuna Capital (submitting or co-filing seven proposals). Twelve companies sought to exclude climate transition proposals, and seven were successful. Another 27 proposals were withdrawn or otherwise did not appear in the company's proxy statement. Of the remaining 17 proposals, 15 had been voted on as of June 1, 2024 and received average support of 23.6%, with none garnering majority support.

2. Continued Focus on GHG Emissions

There were 36 proposals submitted related to measuring GHG emissions or adoption of GHG emissions reduction targets, typically in alignment with the Paris Agreement and often time-bound and covering all three scopes of emissions. Twenty-four of these proposals went to a vote, receiving average support of 28.0%, with two receiving majority support. Five companies sought to exclude GHG emissions proposals via no-action request. Four requests were successful, all under the argument that they improperly micromanaged the company, and the remaining request was withdrawn.

3. Recycling

In 2024, there were 22 proposals submitted related to recycling, plastic waste, or sustainable packaging. The majority of these proposals (13 in total) were submitted or co-filed by As You Sow. Another frequent filer was Green Century Capital Management, submitting eight of these proposals but later withdrawing all but one. No company successfully excluded a recycling proposal in 2024, and 13 were included in companies' proxy statements. Ten recycling proposals had been voted on as of June 1, 2024, averaging 14.0% support with none having received majority support.

4. Other Environmental Proposals

There were 31 "other" environmental proposals unrelated to climate change, recycling, or animal welfare. These proposals varied widely in subject matter, with notable subjects including biodiversity impacts (six proposals), water risks (four proposals) and deforestation in supply chains (four proposals). Five environmental proposals (two related to biodiversity impacts, one related to mining risks, and two anti-ESG proposals) were excluded via no-action requests, three on ordinary business grounds, one on procedural grounds, and one on resubmission grounds. Of the remaining 28 proposals, 15 were withdrawn or otherwise not included in the company's proxy statement and 13 were voted on. Of the eight proposals voted on as of June 1, 2024, two related to sustainable sourcing and supply chain risk; two related to biodiversity impacts; one related to deep-sea mining; one related to lead-sheathed cables; one related to an environmental justice report; and one related to deforestation. None of these proposals received majority support, with support averaging 11.9%.

D. Simple Majority Vote (Eliminate Supermajority Voting)

One of the most frequent proposals submitted requested a simple majority vote (which includes eliminating supermajority vote requirements). Fifty-one proposals were submitted in 2024, a marked increase from 16 in 2023. Simple majority vote proposals generally received significant shareholder support, with 38 going to a vote, averaging support of 70.4%, and 27 receiving majority support. Twelve companies filed no-action requests to exclude these proposals, of which six were successful, five were unsuccessful, and one was withdrawn. While three of the successful no-action requests were based on procedural grounds, three were based on substantial implementation grounds given the specific wording of those proposals. The primary proponent of these proposals was John Chevedden, who filed or co-filed 47 of the 51 proposals.

E. A New Governance Topic: Majority Voting Director Resignation Bylaws

Companies received 46 proposals focused on majority voting director election resignation bylaws in 2024. These proposals, which were a new proposal topic, requested that the company implement a director resignation bylaw that would require each director nominee to submit an irrevocable resignation in the event the director nominee fails to receive majority support and require the company's board of directors to accept the resignation unless it finds a "compelling reason or reasons" not to accept the resignation. In addition, if the resignation is not accepted and the director remains as a "holdover" director, the director resignation bylaw would require that the director's resignation become automatically effective if the "holder" director fails to be re-elected at the next annual meeting. Companies filed 31 no-action requests to exclude these proposals, of which 19 were successful, eight were withdrawn, and four were unsuccessful. The primary reason cited in successful challenges was that the proposal violated state law. Only 12 proposals were voted on, receiving average support of 17.2%, with ISS recommending votes "against" all 12 proposals. All but eight of these 46 proposals were submitted by one of four Carpenter's Pension Funds (New York City, North Atlantic States, Mid-America, or Eastern Atlantic).

F. Advance Notice Bylaws

For the second year in a row, shareholder proponents focused on company advance notice bylaw requirements, expressing concern that bylaw requirements could be used to make it burdensome for shareholders to nominate directors. Whereas the proposals submitted in the 2023 proxy season sought to require shareholder approval of certain advance notice bylaw amendments, the 20 shareholder proposals submitted in 2024, primarily by James McRitchie and the Oregon State Treasury office, sought assurances that companies will treat shareholder nominees equitably. All but one of these proposals were withdrawn, with companies generally addressing the topic in their corporate governance guidelines or proxy statements. At the one company where the proposal was submitted for a vote, ISS recommended votes "against" the proposal and the proposal received only 1.4% of the vote.

V. OTHER IMPORTANT TAKEAWAYS FROM THE 2024 PROXY SEASON

A. *Legal Challenges to the Rule 14a-8 Process*

1. ExxonMobil Litigation over Shareholder Proposal Dismissed, but Could Impact 2025 Proxy Season

In January 2024, Exxon Mobil Corp. (“ExxonMobil”) filed a complaint in federal court in Texas seeking a declaratory judgment that it could exclude a climate change shareholder proposal submitted by activist investor groups Arjuna Capital and Follow This under Rule 14a-8 for inclusion in its 2024 proxy materials.⁴⁰ The proposal asked ExxonMobil to go “beyond current plans, further accelerating the pace of emission reductions in the medium-term for its greenhouse gas (GHG) emissions across Scope 1, 2, and 3, and to summarize new plans, targets, and timetables.” In its complaint, the company accused the activists of being driven by an “extreme agenda,” stated that the proposal “does not seek to improve ExxonMobil’s economic performance or create shareholder value,” and argued that the proposal was excludable under both the SEC’s ordinary business exception and the resubmission exception, the latter of which applies where a substantially similar proposal previously received a low level of shareholder support.

Bringing suit to exclude a shareholder proposal is unusual, as companies typically rely on the no-action request process for relief. ExxonMobil’s complaint also focused on the Staff’s application of Rule 14a-8, noting that changes in Staff interpretations have likely caused a significant increase in the number of proposals submitted and voted on in the last two years, and that the costs of addressing a single shareholder proposal can be high.

The defendants, U.S.-based Arjuna Capital and Netherlands-based Follow This, responded by withdrawing the proposal and arguing that the litigation was moot because they had agreed not to propose it again in the future. ExxonMobil countered that the case should proceed as the proponents could introduce a similar proposal next year despite a history of investors rejecting their proposals. On May 22, 2024, the court ruled on jurisdictional grounds that Exxon could continue its case against Arjuna Capital because Arjuna Capital is a U.S.-based firm but held that it could not hear the claim against Netherlands-based climate activist group Follow This because it lacked jurisdiction over the group. On June 17, 2024, the court subsequently dismissed the remaining claims against Arjuna Capital because Arjuna Capital pledged not only that it would not submit the same proposal again, but that it would not submit similar proposals to ExxonMobil in the future.

⁴⁰ Gibson Dunn was one of the law firms representing ExxonMobil in this matter.

ExxonMobil’s decision to challenge the proposal in court instead of through the typical no-action request process generated several “vote no” campaigns against ExxonMobil’s directors at its 2024 annual meeting, including opposition from large pension funds such as the California Public Employees Retirement System (CalPERS). Despite the organized campaigns launched in response to ExxonMobil’s litigation, all ExxonMobil directors were re-elected at the annual meeting, with support for the company’s slate of directors ranging from 87% to 98% of votes cast, compared with 91% to 98% support in 2023.

2. Impact of Ongoing Shareholder Proposal Litigation at Fifth Circuit Still Uncertain

As discussed in detail in our 2023 update,⁴¹ the 2023 proxy season saw a new challenge to the Staff’s role in the shareholder proposal process emerge in a lawsuit filed by NCPPR in the U.S. Court of Appeals for the Fifth Circuit arising from the Staff’s concurrence with the exclusion on ordinary business grounds of a proposal submitted to The Kroger Co. requesting that the company issue a report “detailing the potential risks associated with omitting ‘viewpoint’ and ‘ideology’ from its written equal employment opportunity (EEO) policy.”⁴² Notably, the Fifth Circuit has, in recent decisions, signaled its willingness to entertain challenges to the SEC’s rulemaking authority.

In *National Center for Public Policy Research v. SEC*, the Fifth Circuit is being asked to address several important questions about the Rule 14a-8 process, including: (1) whether responses to no-action requests issued by the Staff to companies that concur that a company may properly exclude a proposal under Rule 14a-8 are subject to judicial review; (2) the scope of the ordinary business exception under Rule 14a-8(i)(7); and (3) whether Rule 14a-8’s requirement that, absent an exception, companies include shareholder proposals in their proxy statements exceeds the SEC’s authority under the Exchange Act or violates the First Amendment.⁴³

After the Fifth Circuit referred the case to the merits panel (the judicial panel deciding the substantive merits of the complaint), Kroger filed its definitive proxy materials, which included NCPPR’s shareholder proposal.⁴⁴ Subsequently, the NAM intervened in the litigation and raised a far-reaching challenge to the existing Rule 14a-8 framework, arguing that the requirement under Rule 14a-8 that companies include shareholder proposals in their proxy statements (absent an exception) exceeds the SEC’s authority

⁴¹ Shareholder Proposal Developments During the 2023 Proxy Season (July 25, 2023) (“2023 Shareholder Proposals Update”), available [here](#).

⁴² *The Kroger Co.* (avail. Apr. 12, 2023).

⁴³ The case arose out of a proposal submitted to The Kroger Co. requesting that the company issue a report “detailing the potential risks associated with omitting ‘viewpoint’ and ‘ideology’ from its written equal employment opportunity (EEO) policy.” The Staff concurred with Kroger’s no-action request, which argued that NCPPR’s proposal could be excluded on ordinary business grounds. In response, NCPPR filed a petition for review of the Staff’s no-action decision in the Fifth Circuit and asked the court to stay the no-action decision during the litigation.

⁴⁴ NCPPR initially also sued Kroger in federal district court but dropped its lawsuit once the company agreed to include the proposal in its proxy statement. NCPPR’s proposal was voted on at Kroger’s 2023 annual meeting and received only 1.9% support.

under the Exchange Act and asserting that the statutory provision only authorizes the SEC to target misleading or deceptive statements by a company in its proxy statement. NAM further argued that, if Rule 14a-8 is statutorily authorized, it violates the First Amendment because the rule requires companies to speak on controversial topics and alters the content of their speech in contravention of the Constitution's restrictions on compelled speech and content-based speech regulations.

Notably, contrary to concerns that the pending litigation could impact the Staff's willingness to entertain no-action requests on purportedly similar proposals or arguing for exclusion on the basis of ordinary business, the Staff did not decline to respond to ordinary business no-action requests.⁴⁵ Accordingly, the ultimate impact of NCPPR's litigation will likely turn on the Fifth Circuit's ruling.

Most recently, the Fifth Circuit merits panel heard arguments in the case in March 2024, but it is unclear when the Fifth Circuit will issue its decision.

B. Novel Shareholder Proposal Tactic Building on Universal Proxy

As part of the universal proxy rule amendments, the SEC amended Rule 14a-4(d) to allow anyone to solicit votes for or against a company's director candidates without the consent of those directors, which previously was not permissible. This amendment means that if a dissident solicits proxies to vote on shareholder proposals presented at a company's shareholders' meeting other than pursuant to Rule 14a-8 (referred to as "floor proposals"), that dissident can now include the election of directors on its own proxy card that includes its floor proposals.⁴⁶ Relying on this rule change, and foreshadowing a possible new tactic to avoid the limitations of Rule 14a-8, the AFL-CIO and United Mine Workers of America submitted five non-binding shareholder proposals under Warrior Met Coal, Inc.'s advance notice bylaws instead of under Rule 14a-8, and subsequently satisfied the conditions of Rule 14a-4(c)(2)⁴⁷ by filing their own proxy materials, including their own proxy card, and sending their proxy materials to shareholders owning at least 50% of the company's stock. The AFL-CIO and United Mine Workers indicated in their proxy materials that the total cost for their solicitation was estimated to be only \$15,000. The AFL-CIO and United Mine Workers included Warrior Met Coal's director slate on their proxy card (although they did not nominate any directors or make a voting recommendation as to the directors), along with management's proposals and the five non-binding shareholder proposals, and, because

⁴⁵ The Staff took this approach, for example, in the early 1990s during litigation involving the application of the ordinary business exception to shareholder proposals requesting implementation of nondiscrimination policies, and more recently during the 2015 proxy season while the SEC was reconsidering the application of the conflicting proposals exception in Rule 14a-8(i)(9).

⁴⁶ The amendment to Rule 14a-4(d) also means that dissidents can actively solicit proxies to vote against company director nominees in a "vote no" campaign, which occurred at several companies during the 2024 proxy season.

⁴⁷ Under Rule 14a-4(c)(2), if a proponent who plans to introduce a floor proposal satisfies certain conditions, including filing and sending its own proxy statement and proxy card to shareholders owning sufficient shares to approve its proposal, the company needs to include that proposal as a separate voting item in its proxy statement and on its proxy card if it wishes to use proxies solicited from shareholders to vote on the floor proposal.

the AFL-CIO and United Mine Workers satisfied 14a-4(c)(2), Warrior Met Coal needed to include all five of the AFL-CIO and United Mine Workers proposals (but not a supporting statement by the shareholders) in its proxy statement and on its proxy card so that it could solicit votes against the proposals.

The proposals submitted by the AFL-CIO and the United Mine Workers, which had been in collective bargaining negotiations with Warrior Met Coal for the past three years, raised typical corporate governance issues usually addressed under Rule 14a-8 (four proposals covered various corporate governance matters, including shareholder approval of poison pills, blank-check preferred stock, golden parachutes, and proxy access, and a fifth proposal requested an assessment of Warrior Met Coal's respect for the human rights of freedom of association and collective bargaining).

Warrior Met Coal supported the proxy access shareholder proposal but opposed the other shareholder proposals. ISS recommended shareholders vote for all of Warrior Met Coal's proposals, including its director nominees, and for all but two of the shareholder proposals (the proposals related to shareholder approval blank-check preferred stock and golden parachutes). The proxy access and poison pill proposals received majority support, while the other three shareholder proposals failed (although the shareholder proposal requesting an assessment related to labor matters received support from 46% of votes cast).

C. Stalemate at the SEC and Congress on Rule 14a-8 Regulatory Change

1. SEC Amendment of Rule 14a-8

As discussed in our 2023 update,⁴⁸ the SEC proposed significant amendments to Rule 14a-8 in July 2022 (the "2022 Proposed Amendments"). If adopted, the 2022 Proposed Amendments would formally modify three substantive bases for exclusion of shareholder proposals—substantial implementation, duplication, and resubmission.⁴⁹ In keeping with the thrust of SLB 14L and the Staff's more restrictive interpretations of Rule 14a-8's exclusions since 2021, the 2022 Proposed Amendments would have the effect of further limiting the availability of these grounds for exclusion, likely leading to more shareholder proposals going to a vote.

After initially targeting adoption of the 2022 Proposed Amendments by October 2023, the SEC has once again postponed its target date. According to the SEC's Spring 2024 Unified Agenda of Regulatory and Deregulatory Actions (the "Reg Flex Agenda") released on July 7, 2024,⁵⁰ the SEC is now targeting adoption of the 2022 Proposed Amendments by April 2025. With the 2024 U.S. elections looming, whether the 2022 Proposed Amendments are adopted and go into effect will likely turn on the outcome of the Presidential election. Moreover, in light of the Supreme Court's overruling *Chevron*

⁴⁸ 2023 Shareholder Proposals Update.

⁴⁹ See Release No. 34-95267 (the "2022 Proposing Release"), available [here](#).

⁵⁰ *Agency Rule List – Spring 2024 Securities and Exchange Commission, Office of Information and Regulatory Affairs* (2024), available [here](#).

deference,⁵¹ the SEC likely will face a challenge to its authority to use Rule 14a-8 to regulate shareholder proposals if it proceeds with amending the rule.

2. Congressional Efforts to Reform Rule 14-8 Appear to Have Stalled

Congressional efforts to reform Rule 14a-8 appear to have been put on the backburner in the run-up to the 2024 elections. As discussed in last year's update,⁵² the House Financial Services Committee Chairman Patrick McHenry (R-NC) announced in 2023 the formation of a Republican ESG Working Group, comprised of nine members and led by Representative Bill Huizenga (R-MI), "to combat the threat to our capital markets posed by those on the far-left pushing environmental, social, and governance (ESG) proposals."⁵³ The Working Group was established to "[r]eign in the SEC's regulatory overreach; [r]einforce the materiality standard as a pillar of our disclosure regime; [a]nd hold to account market participants who misuse the proxy process or their outsized influence to impose ideological preferences in ways that circumvent democratic lawmaking." Among its key priorities is reforming the Rule 14a-8 no-action request process, which the Working Group argues is now "a mechanism for SEC staff to project its views about the 'significance' of non-securities issues, rather than a process for ensuring shareholder proponents' interests are aligned with those of their fellow shareholders."

In July 2023, Representative Bryan Steil (R-WI) introduced H.R. 4767, the Protecting Americans' Retirement Savings from Politics Act,⁵⁴ which would, among other things, (1) raise the resubmission thresholds for shareholder proposals under Rule 14a-8(i)(12), (2) nullify the 2022 Proposed Amendments, (3) permit companies to exclude a proposal if "the subject matter of the shareholder proposal is environmental, social, or political (or a similar subject matter)," and (4) permit companies to exclude proposals that implicate ordinary business matters under Rule 14a-8 regardless of whether they relate to a "significant social policy issue." H.R. 4767 was referred to the full House of Representatives but has yet to be brought to a vote. On September 27, 2023, the House Financial Services Committee held a hearing entitled "Oversight of the Securities and Exchange Commission," with Chair Gensler testifying. The hearing, which was held to "examine the regulatory developments, rulemakings, and activities that the SEC has undertaken in the period since October 5, 2021," covered the 2022 Proposed Amendments.⁵⁵ However, the Working Group's push to reform Rule 14a-8 appears to

⁵¹ See, *Loper Bright Enterprises v. Raimondo* (June 28, 2024), discussed in our update *Supreme Court Overrules Chevron, Sharply Limiting Judicial Deference To Agencies' Statutory Interpretation* (June 28, 2024), available [here](#). The Supreme Court's ruling in *Corner Post v. Board of Governors, Federal Reserve System* (July 1, 2024), holding that the Administrative Procedure Act's statute of limitations runs from when an agency rule injures the plaintiff, not when the agency issues the rule, may also support increased challenges to Rule 14a-8.

⁵² Available [here](#).

⁵³ Press Release, *McHenry Announces Financial Services Committee Republican ESG Working Group* (Feb. 3, 2023), available [here](#).

⁵⁴ Available [here](#).

⁵⁵ *Memorandum re September 27, 2023, Full Committee Hearing* (September 22, 2023), available [here](#).

have stalled, and Rep. Huizenga has acknowledged in interviews that the anti-ESG bills advanced by the Working Group are unlikely to advance further.⁵⁶

D. Shareholders Continue to Use Exempt Solicitations

The use of exempt solicitation filings by shareholder proponents increased slightly in 2024, including as part of efforts to generate greater publicity for their proposals in advance of shareholder meetings or to address other topics. Under Rule 14a-6(g) under the Exchange Act, shareholders owning more than \$5 million of a company's securities generally must file a Notice of Exempt Solicitation (an "Exempt Notice") on EDGAR when soliciting other shareholders to vote on a proposal without seeking to act as a proxy. The rule is one of several exempting certain solicitations from the proxy filing requirements, and it was designed to address concerns that institutional investors and other large shareholders would conduct "secret" solicitations. However, in recent years, these filings have primarily been used by smaller shareholders and shareholder representatives to publicize their views on various proposals, as the Staff does not restrict their use of these filings. In this regard, approximately 68% of Exempt Notices filed in 2024 were identified as voluntary filings by shareholders who did not own more than \$5 million in company stock, down slightly from 71% from 2023. As a result, it seems that shareholders continue to use these filings outside of Rule 14a-6(g)'s intended scope, resulting in some compliance issues and potential confusion for other shareholders when evaluating the items to be voted on.

As of June 1, 2024, there were a record-high 357 Exempt Notices filed since the beginning of the calendar year, up slightly from 347 as of the same date in 2023 and 285 as of the same date in 2022. Frequent filers included As You Sow with 44 filings (down from 48 in 2023), Bowyer Research, Inc. with 41 filings (up from zero in 2023), John Chevedden with 28 filings (level with 2023), the National Legal and Policy Center ("NLPC") with 22 filings (down from 29 in 2023), and Inspire Investing, LLC with 22 filings (up from zero in 2023). These top five filers were responsible for almost 44% of all Exempt Notices during the calendar year. Several proponents who filed numerous Exempt Notices in 2023 significantly reduced the number of their filings in 2024, such as New York State Common Retirement Fund with seven filings (down from 18 in 2023) and Majority Action, LLC with three filings (down from 16 in 2023). All of the Exempt Notices filed by As You Sow, John Chevedden, and NLPC, were voluntary, while neither Bowyer Research, Inc. nor Inspire Investing, LLC (who were both new to Exempt Filings) designated their filings as either voluntary or mandatory.

In 2023, we first identified a trend by which intervening third parties filed Exempt Notices to publicly express their views on shareholder proposals submitted by shareholder proponents with whom they have no apparent relationship. That trend continued in 2024, particularly among anti-ESG advocates. For example, 17 of Inspire Investing, LLC's 22 Exempt Notices were filed in support of proposals submitted by other shareholder proponents, such as a proposal submitted by NCPPR at Salesforce, Inc. requesting a report on risks related to denying or restricting service to users or

⁵⁶ See David Hood, *Anti-ESG House Bills Struggle to Clear Competing GOP Priorities*, Bloomberg, Nov. 17, 2023, available [here](#).

customers⁵⁷ and the proposal jointly submitted by Bowyer Research and The Bahnsen Family Trust at Walmart Inc. requesting a report on how the company’s policies and practices impact employees and prospective employees based on their religion or political views.⁵⁸ As in prior years, various anti-ESG organizations also submitted Exempt Notices to urge shareholders to vote against various proposals. For example, Bowyer Research filed an Exempt Notice urging shareholders to vote against a proposal requesting a report on the implementation of Tripadvisor, Inc.’s Global Human Rights Policy submitted by Mercy Investment Services, The Episcopal Church and Portico Benefit Services.⁵⁹ Bowyer Research also filed Exempt Notices to lobby against proposals submitted at a number of companies, including Lockheed Martin Corp., HP Inc., Starbucks Corp., and Intuit Inc. Notably, several of Bowyer Research’s Exempt Notices did not advocate for any particular vote by shareholders—instead they were general whitepapers on issues such as political activism and shareholder value.⁶⁰

Despite the continued growth in the use of Exempt Solicitations, the Staff has continued to avoid addressing the potential for abuse. That potential abuse may be compounded if intervening third parties, who may or may not be shareholders, continue to use Exempt Notices to support or oppose shareholder proposals submitted by shareholder proponents or, as we saw this year, use Exempt Notices for general advocacy purposes not directly related to a specific shareholder proposal.⁶¹ We continue to recommend that companies actively monitor their EDGAR file for these filings, review any Exempt Notices carefully, and inform the Staff to the extent they believe an exempt solicitation filing contains materially false or misleading information or may not have been filed by a shareholder.⁶²

⁵⁷ Available [here](#).

⁵⁸ Available [here](#).

⁵⁹ Available [here](#).

⁶⁰ For example, see the Exempt Notices filed at The Walt Disney Co. and Starbucks Corp., *available [here](#) and [here](#), respectively*.

⁶¹ Unlike Exempt Notices filed by shareholder proponents, who were required to provide proof of their shareholder status when submitting their shareholder proposals, companies may be unable to confirm whether the intervening third parties are actually shareholders eligible to file Exempt Notices under Rule 14a-6(g).

⁶² In 2018, the Staff published two new Compliance and Disclosure Interpretations (“C&DIs”) providing some guidance on the use of Exempt Notices. Question 126.06 confirms the Staff’s view that “voluntary” Notices of Exempt Solicitations can be filed, and Question 126.07 clarifies that each Notice of Exempt Solicitation, whether filed voluntarily or because it is required under Rule 14a-6(g), must include a notice page setting forth the information required under Rule 14a-103. Both C&DIs are available [here](#).

E. Practice Pointers for the 2025 Proxy Season and Beyond

While the 2024 proxy season is just now concluding, companies should begin preparations for the 2025 proxy season now.

- **Monitor the Legal, Regulatory and Investment Landscape.** While regulatory change is unlikely to come prior to the November 2024 election, as we saw following the 2020 election, changes in Presidential administration and leadership at the SEC can bring abrupt changes to the shareholder proposal process. Companies should continue to monitor legislative, judicial, and other legal developments that may impact shareholder proposals heading into the 2025 proxy season. In addition, companies should be mindful to familiarize themselves with the proxy voting and other governance policies released by proxy voting firms and major institutional investors, particularly as members of the investment community issue updated policies and guidance in the run up to the 2025 proxy season.
- **Don't Shy Away from the No-Action Request Process.** Given the success of no-action requests during the 2024 proxy season, companies should be sure to carefully consider whether there are substantive bases (in addition to procedural grounds) for challenging any proposals received for the 2025 proxy season.
- **When Submitting No-Action Requests, Be Mindful of Staff Review Times.** As part of its efforts to modernize the Rule 14a-8 no-action request submission process, the Staff introduced an online portal through which all no-action requests and related correspondence must be submitted. Although Rule 14a-8 requires a company to submit no-action requests at least 80 calendar days prior to the date it intends to file its definitive proxy materials, the portal requires companies to advise the Staff of its anticipated deadline to print its proxy materials in order to help facilitate timely responses. In 2024, the average Staff no-action request response time, excluding withdrawals, was 64 calendar days. Companies should factor this extended time period into proxy timelines and be sure to keep the Staff apprised of any changes to their printing and filing deadlines to help ensure Staff responses are timely received.
- **Mind the Ps and Qs of Procedural Challenges.** While the 2024 proxy season saw a decline in success rates for procedural no-action requests (68% in 2024, compared with 80% in 2023), they still represented 29% of successful requests. As such, companies should continue to carefully review shareholder proposals received and raise identified deficiencies in timely delivered deficiency notices that provide clear, plain English explanations of any identified procedural deficiencies.
- **Be Ready for Proposals Submitted Under Advance Notice Bylaws.** As the developments at Warrior Met Coal demonstrate, shareholders now have a more viable alternative to Rule 14a-8 that is supported by the recent amendments to Rule 14a-4. While it remains to be seen if more proponents incur the time and expense to take the Rule 14a-4 floor proposal route to avoid the requirements and limitations of Rule 14a-8, companies should be ready to respond

expeditiously to the submission of proposals under their advance notice bylaws going forward, including preparing a checklist of requirements under their advance notice bylaws.

The following Gibson Dunn attorneys assisted in preparing this update: Aaron Briggs, Elizabeth Ising, Julia Lapitskaya, Ronald O. Mueller, Michael Titera, Lori Zyskowski, Geoffrey Walter, Victor Twu, Natalie Abshez, Meghan Sherley, Nicholas Whetstone, Chad Kang, Nathan Marak, Antony Nguyen and Jack Strachan.

Gibson Dunn's lawyers are available to assist with any questions you may have regarding these developments. To learn more about these issues, please contact the Gibson Dunn lawyer with whom you usually work, or any of the following lawyers in the firm's Securities Regulation and Corporate Governance practice group:

*Aaron Briggs – San Francisco, CA (+1 415-393-8297, abriggs@gibsondunn.com)
Elizabeth Ising – Washington, D.C. (+1 202-955-8287, eising@gibsondunn.com)
Thomas J. Kim – Washington, D.C. (+1 202-887-3550, tkim@gibsondunn.com)
Julia Lapitskaya – New York, NY (+1 212-351-2354, jlapitskaya@gibsondunn.com)
Ronald O. Mueller – Washington, D.C. (+1 202-955-8671, rmueller@gibsondunn.com)
Michael Titera – Orange County, CA (+1 949-451-4365, mtitera@gibsondunn.com)
Lori Zyskowski – New York, NY (+1 212-351-2309, lzyskowski@gibsondunn.com)
Geoffrey E. Walter – Washington, D.C. (+1 202-887-3749, gwalter@gibsondunn.com)
David Korvin – Washington, D.C. (+1 202-887-3679, dkorvin@gibsondunn.com)*

Considerations for Preparing Your 2023 Form 10-K

Client Alert | December 1, 2023

An annual update of observations on new developments and highlights of considerations for calendar-year filers preparing Annual Reports on Form 10-K. Each year we offer our observations on new developments and highlight select considerations for calendar-year filers as they prepare their Annual Reports on Form 10-K. This alert touches upon recent rulemaking from the U.S. Securities and Exchange Commission (“SEC”), comment letters issued by the staff of the SEC’s Division of Corporation Finance (the “Staff”), and trends among reporting companies that have emerged throughout the last year. An index of the topics described in this alert is provided below. [I. New Disclosure Requirements for 2023](#) [A. Update on Repurchase Rule](#) [B. Cybersecurity Risk Management, Strategy, and Governance Disclosures](#) [1. Risk Management and Strategy](#) [2. Governance](#) [C. Rule 10b5-1 Plan Disclosures for Section 16 Officers and Directors](#) [D. Compensation Clawback Disclosures](#) [II. Disclosure Trends and Considerations](#) [A. Climate Change](#) [B. Human Capital](#) [C. Generative Artificial Intelligence](#) [D. Geopolitical Conflict](#) [E. Potential Government Shutdown](#) [F. Inflation and Interest Rate Concerns](#) [III. SEC Comment Letter Trends](#) [IV. Other Reminders and Considerations](#) [A. Disclosure Controls and Procedures](#) [B. Characterization of Legal Proceedings](#) [C. EDGAR Next](#) [D. Filing Requirement for “Glossy” Annual Report](#) [E. Cover Page XBRL Disclosures](#) **I. New Disclosure Requirements for 2023** Throughout 2023, the SEC has maintained the rapid pace of rulemaking we have seen since Chair Gary Gensler took office in 2021. New disclosure requirements that, for calendar year-end companies, will begin to apply for the first time with the 2023 Form 10-K consist of:

- Cybersecurity risk management, strategy, and governance disclosures, which will be included under “Item 1C. Cybersecurity,” a new caption under Part I; and
- Compensation clawback-related disclosures, which involve a new Exhibit 97, two new checkbox disclosures on the Form 10-K cover page, and disclosure in Part III, “Item 11. Executive Compensation,” which most companies will forward-incorporate by reference to their upcoming proxy statements.

Beginning with the 2024 Form 10-K next year, all of the new cybersecurity disclosure requirements will need to be tagged in Inline XBRL (“iXBRL”). Rules that would have required new disclosures around company share repurchases and company Rule 10b5-1 plans were challenged in litigation and therefore appear unlikely to apply to companies’ 2023 Forms 10-K. Set forth below are discussions of each of the new disclosure requirements. **A. Update on Repurchase Rule** On November 22, 2023, the SEC [announced](#)[1] that it had issued an order indefinitely postponing the effectiveness of the Share Repurchase Disclosure Modernization rule (the “Repurchase Rule”), pending further SEC action. At the same time, the SEC asked the Fifth Circuit for additional time to respond to the court’s order, discussed below, requiring the SEC to correct deficiencies in the Repurchase Rule by November 30, 2023. The petitioners in the lawsuit that had challenged the Repurchase Rule opposed the SEC’s motion and requested instead vacatur of the Repurchase Rule. The court denied the SEC’s motion on November 26, 2023. We will provide further updates on the Repurchase Rule in the [Gibson Dunn Securities Regulation Monitor](#). [2] The Repurchase Rule, discussed in our client alert [here](#)[3], requires companies to: (i) disclose daily company share repurchase data in a new table filed as an exhibit to reports on Form 10-Q and Form 10-K, (ii) provide narrative disclosure in those filings about the company’s share repurchase program, including its

Related People

[Ronald O. Mueller](#)

[Elizabeth A. Ising](#)

[Michael A. Titera](#)

[David Korvin](#)

[Meghan Sherley](#)

[Victor Twu](#)

[Maggie Valachovic](#)

[Nathan Marak](#)

[Michael Scanlon](#)

[Julia Lapitskaya](#)

objectives and rationale, and referencing the particular repurchases that correspond to that narrative, (iii) indicate by a checkbox whether any executives or directors traded in the company's equity securities within four business days before or after the public announcement of the repurchase plan or program or the announcement of an increase of an existing share repurchase plan or program, and (iv) provide quarterly disclosure regarding the company's adoption or termination of any Rule 10b5-1 trading arrangements. The Repurchase Rule was scheduled to go into effect beginning with the Form 10?K or Form 10-Q filed for the first full fiscal quarter beginning on or after October 1, 2023, meaning that for calendar year-end companies, these disclosure requirements would have applied to the 2023 Form 10-K. While the Repurchase Rule is stayed, the pre-existing share repurchase disclosure rules, requiring information on share repurchase programs and quarterly repurchase disclosures presented on an aggregated, monthly basis, remain in effect. In addition, as discussed in Section I.C below, companies must continue to satisfy the Rule 10b5-1 plan disclosure requirements for Section 16 officers and directors.

B. Cybersecurity Risk Management, Strategy, and Governance

Disclosures On July 26, 2023, the SEC adopted a suite of new cybersecurity disclosure requirements, which we discussed in our client alert available [here](#).^[4] In addition to the incident disclosure requirements on Form 8-K, the final rule includes a number of new disclosure items on Form 10-K regarding cybersecurity risk management, strategy, and governance under new Item 106 of Regulation S-K. Companies are required to comply with these disclosure requirements beginning with the Form 10-K for the first fiscal year ending on or after December 15, 2023, which for calendar year-end companies is the 2023

1. Risk Management and Strategy Under new Item 106, companies are required to describe their processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. The definitions of cybersecurity incident and cybersecurity threat extend to all information systems a company uses, not just those the company itself owns. In providing such disclosure, a company should address, as applicable, the following non-exclusive list of disclosure items:

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

Companies must also describe whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the company, including its business strategy, results of operations, or financial condition and if so, how. While discussing the board's role in company-wide risk oversight is familiar for public companies, this new requirement goes further and requires that companies delve more deeply into the company's efforts to assess, identify and manage this one particular area of risk. As such, compliance with the rules will require coordination with personnel responsible for day-to-day cybersecurity risk management.

2. Governance Companies must describe the board of directors' oversight of risks from cybersecurity threats. If applicable, companies must identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the processes by which the board or such committee is informed about such risks. In addition, companies must describe management's role in assessing and managing the company's material risks from cybersecurity threats, with such disclosure addressing, as applicable, the following non-exclusive list of disclosure items:

- Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise;
- The processes by which such persons or committees are informed about and

monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and

- Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.

With respect to management's expertise, the instructions to Item 106 provide that it may include "[p]rior work experience in cybersecurity; any relevant degrees or certifications; any knowledge, skills, or other background in cybersecurity." Interestingly, with this requirement, the SEC is seeking a level of detail regarding cybersecurity executives' backgrounds that is not even required for chief executive officers or chief financial officers. Companies will need to think through how much detail is "necessary to fully describe the nature of the expertise" of its chief information security officer or other cybersecurity personnel. As noted by the SEC, many companies currently address cybersecurity risks and incidents in the risk factor sections of their filings, and risk oversight and governance are often addressed in companies' proxy statements. However, the new rule requires disclosures to appear in a newly designated Item 1C in Part I of the Form 10-K and does not allow the disclosures to be incorporated from the proxy statement. Companies should review their risk factor and proxy statement disclosures when drafting the new discussions of cybersecurity risk management, strategy, and governance in order to maintain consistency with the company's past public statements regarding its cybersecurity risks governance and processes and to assess how those disclosures may be conformed or enhanced going forward. We expect companies will continue to include disclosure of cybersecurity governance in their proxy statements, and therefore should confirm that they are using terminology consistently across the documents and should consider whether any details disclosed under the new requirements should be repeated in the proxy statement disclosure. Companies should note that, beginning with the Form 10-K next year (2024 for calendar year-end companies), all of the new disclosure requirements will need to be tagged in iXBRL (block text tagging for narrative disclosures and detail tagging for quantitative amounts). **C.**

Rule 10b5-1 Plan Disclosures for Section 16 Officers and Directors On December 14, 2022, the SEC adopted a final rule introducing disclosure requirements with respect to the adoption or termination of Rule 10b5-1 plans by Section 16 officers and directors, which we discussed in more detail in our client alert available [here](#).^[6] In Form 10-K and Form 10-Q, companies must disclose whether any Section 16 officer or director adopted or terminated a Rule 10b5-1 plan or a "non-Rule 10b5-1 trading arrangement" during the prior quarter. Amended Rule 10b5-1 now specifically states that any modification or amendment to an existing trading plan to change the amount, price, or timing of the purchase or sale of the securities underlying the plan would be deemed termination of a plan and entry into a new plan, and would therefore trigger disclosure in the Form 10-K or Form 10-Q covering the quarter in which the plan was modified or amended. For all companies but smaller reporting companies ("SRCs"), the requirement became effective with the filing covering the first full fiscal quarter that began on or after April 1, 2023. SRCs are required to comply with the requirement beginning with the filing covering the first full fiscal quarter beginning on or after October 1, 2023, which for calendar year-end SRCs is the 2023 Form 10-Q. As noted above, the Repurchase Rule would have required disclosure of the same type of information regarding companies' adoption or termination of Rule 10b5-1 plans, but the requirement has not taken effect. For each trading arrangement that is adopted or terminated, the disclosure must identify whether the trading arrangement is a Rule 10b5-1 plan or a non-Rule 10b5-1 trading arrangement, and provide a brief description of the material terms (other than price), including (i) the name and title of the director or officer; (ii) the date of adoption or termination of the trading arrangement; (iii) the duration of the trading arrangement; and (iv) the aggregate number of securities to be sold or purchased under the trading arrangement (including pursuant to the exercise of any options). As discussed in our previous post, the form of this disclosure is not prescribed by the final rule.^[7] While the vast majority of companies we surveyed have provided narrative disclosure in response to the requirement, a minority have provided tabular disclosure instead. For an example of this narrative disclosure, please see our prior post regarding the new insider trading rules.^[8] While companies have taken

a varied approach to this disclosure when no Section 16 officers or directors have adopted or terminated Rule 10b5-1 plans during the quarter, we note that the majority of companies we surveyed have chosen to include narrative disclosure that states there have been no such adoptions or terminations (e.g., “During the quarter ended [date], no director or officer (as defined in Rule 16a-1(f) under the Exchange Act) of the Company adopted or terminated any Rule 10b5-1 trading arrangements or non-Rule 10b5-1 trading arrangements (in each case, as defined in Item 408(a) of Regulation S-K).”). Another approach some companies have taken is to simply state “None” under the applicable Item, and a small minority of the companies elected to make no disclosure and to omit the relevant Item from the periodic filing altogether (which is permissible under the instructions to Part II of Form 10-Q, but not permissible in the Form 10-K).

D. Compensation Clawback Disclosures On October 26, 2022, the SEC adopted final rules that require listed companies to implement policies for recovery (i.e., “clawback”) of erroneously awarded incentive compensation.^[9] In addition to disclosures related to the application of the clawback policies, which for most companies will be included in the proxy statement,^[10] there are two disclosure components specific to the Form 10-K that companies must comply with beginning with any Form 10-K filed on or after December 1, 2023, the date by which companies must have adopted the clawback policies. The first component is the addition of two new checkboxes to the Form 10-K cover page, which requires companies to indicate whether (i) the financial statements included in the filing reflect the correction of an error to previously issued financial statements and (ii) any such corrections are restatements that required a recovery analysis pursuant to Rule 10D-1(b). We expect a number of interpretive questions to arise with respect to the applicability of the checkboxes in various contexts. For example, the Staff has informally confirmed that the first checkbox would not need to be checked if the annual financial statements included in the Form 10-K reflect the correction of a material error to *interim* financial statements and where that error only affected the interim periods (but not any *annual* periods).^[11] However, the first box may need to be checked if the 10-K reflects even an immaterial correction to previously issued annual financial statements. The second checkbox only needs to be checked for material error corrections (i.e., a “little r” restatement or “Big R” restatement) that triggered a clawback recovery analysis. The second component is the requirement for companies to file their clawback policy as Exhibit 97 to the Form 10-K.

II. Disclosure Trends and Considerations A. Climate Change The landscape of climate change disclosure requirements continues to evolve with the adoption of the Corporate Sustainability Reporting Directive (“CSRD”) by the European Council in November 2022, which impacts both EU and U.S. companies, and three new laws in California, which impact both public and private companies doing business or operating in California.^[12] Final SEC rules on climate-related disclosure are still pending,^[13] but the SEC has continued to issue Form 10-K comment letters regarding companies’ climate-related disclosures under existing requirements. For companies reviewing their existing climate-related disclosures in their Form 10-K, a few items to consider in light of Staff comments made since the issuance of the SEC’s sample comment letter related to climate change disclosure that it issued in 2021^[14] include:

- Tailor climate-related disclosures to the company’s business and financial condition, rather than generic discussions on climate change. For example, the Staff may ask a company to provide specific disclosure, if material, as to the impact on the company’s business of climate change risks disclosed in the risk factor section. Overly broad statements may also inadvertently create future reporting obligations as legislation, such as California’s Assembly Bill No. 1305, begins to tie disclosure requirements to the making of certain sustainability-related claims.
- Consider whether certain climate-related matters should be disclosed not only qualitatively, but also quantitatively. For example, if climate-related capital projects have become a significant portion of overall capital expenditures spending, the comment letters indicate that quantitative disclosure may be warranted.
- For any climate-related disclosure included in the Form 10-K, take steps to adequately substantiate those disclosures. This involves, among other things,

assessing the methodology and assumptions underlying climate-related disclosures. Companies should be mindful that disclosures made today can carry liability for years to come and give sufficient attention to these disclosures now to avoid liability down the road. Frameworks such as COSO's "Achieving Effective Internal Control Over Sustainability Reporting" and related guidance can be helpful when building or expanding ESG-related internal controls.

- As part of the disclosure controls and procedures for the 2023 Form 10-K filing, review the company's publicly disclosed ESG materials, such as the company's sustainability report, to determine whether any of the information is or may become material under federal securities laws. Based on Staff comments, the Staff has gone outside a company's SEC filings to review ESG-related statements made elsewhere and ask what consideration was given to including such disclosures in the Form 10-K. To the extent information disclosed in sustainability reports is not material for purposes of SEC rules (often, it is not), appropriate disclaimers to that effect should be provided as we previously advised in our prior client alert, "Considerations for Climate Change Disclosures in SEC Reports."[\[15\]](#)

B. Human Capital Since 2021, companies have been required to include in their Form 10-K[\[16\]](#) a description of the company's human capital resources, to the extent material to an understanding of the business taken as a whole, including the number of persons employed by the company and any human capital measures or objectives that the company focuses on in managing the business (such as, depending on the nature of the company's business and workforce, measures or objectives that address the development, attraction and retention of personnel). The rule adopted by the SEC did not define "human capital" or elaborate on the expected content of the disclosures beyond the few examples provided in the rule text. This principles-based approach has resulted in significant variation among companies' disclosures. With three years of human capital disclosure now available, we recently conducted a survey of the substance and form of human capital disclosures made by the S&P 100 in their Forms 10-K for their three most recently completed fiscal years. While company disclosures continued to vary widely, we saw companies continuing to tailor the length of their disclosure and the range of topics covered and also noted a slight increase in the amount of quantitative information provided in some areas. For a more detailed summary of our findings from this survey, which looked at eight primary categories of human capital disclosure, please see our prior client alert, "Form 10-K Human Capital Disclosures Continue to Evolve."[\[17\]](#) While we anticipate that human capital disclosure will continue to evolve under the existing principles-based requirements, the SEC is expected to propose more prescriptive rules that could significantly change the landscape. At its meeting on September 21, 2023, the SEC's Investor Advisory Committee approved subcommittee recommendations to expand required human capital management disclosures, which include prescriptive disclosure requirements (such as headcount of full-time versus part-time and contingent workers, turnover metrics, the total cost of the issuer's workforce broken down into components of compensation, and demographic data of diversity across gender, race/ethnicity, age, disability, and/or other categories) as well as narrative disclosure in management's discussion and analysis of how the company's "labor practices, compensation incentives, and staffing fit within the broader firm strategy."[\[18\]](#)

C. Generative Artificial Intelligence Recent developments in artificial intelligence ("AI"), including generative AI, may accelerate or exacerbate potential risks related to technological developments. Companies should consider ways in which the company's strategy, productivity, market competition and demand for the company's products, investments and the company's reputation, as well as legal and regulatory risks could be affected by AI. Companies should also consider any impacts related to cybersecurity and social or ethical challenges. These updates may affect existing risk factors or merit a new standalone risk factor or mention in the forward-looking statement disclaimer, depending on the importance of AI to the company's business. Further consideration should be given to discussing AI in the business section and trends section of the MD&A, as applicable.

D. Geopolitical Conflict Public companies need to consider the recent and evolving developments in the Middle East in their Form 10-K, including as to whether risks associated with these

developments are adequately discussed in the risk factors, as well as their direct and indirect impacts on their operations and financial condition. While the SEC has not published specific disclosure guidance related to the Middle East, the Staff's "Sample Comment Letter Regarding Disclosures Pertaining to Russia's Invasion of Ukraine and Related Supply Chain Issues"[\[19\]](#) may provide guidance as to the types of disclosure that may be necessary. Companies should consider whether disclosure should be provided, to the extent material, regarding any material impacts or risks related to (i) direct or indirect exposure due to operations or investments in affected countries, securities trading in affected countries, sanctions imposed or legal or regulatory uncertainty associated with operating in or existing in the Middle East, (ii) direct or indirect reliance on goods or services sourced in the Middle East, (iii) actual or potential disruptions in the company's supply chain, or (iv) business relationships, connections to, or assets in the Middle East. Companies should undertake similar disclosure analyses to determine whether direct or indirect impacts of or material risks from the continued conflict between Russia and Ukraine or emerging geopolitical conflicts, such as rising tensions between China and Taiwan and China and the United States, should be discussed in any sections of the upcoming Form 10-K. Companies with operations in the People's Republic of China should review the Division of Corporation Finance's recent sample comment letter[\[20\]](#) highlighting three focus areas for periodic disclosures related to China-specific matters, including those arising from the Holding Foreign Companies Accountable Act (the "HFCAA"), the Uyghur Forced Labor Prevention Act, and specific government-related operational risks. In addition to posing questions regarding HFCAA disclosures, the sample letter includes comments directed at risk factors and MD&A disclosure.

E. Potential Government Shutdown Companies should continue to monitor the potential for a shutdown of the U.S. federal government and consider whether any looming prospect of a shutdown poses new risks for the business. In particular, companies trading in U.S. government securities or other securities with values derived from U.S. government securities should revisit any risk factors or other disclosures related to potential default by the federal government, including discussing any material losses in MD&A or elsewhere. As noted in the SEC Division of Corporation Finance's announcement in September regarding the anticipated impacts of a potential government shutdown, EDGAR will continue to accept filings during a shutdown, so filing Forms 10-K should not be affected.[\[21\]](#)

F. Inflation and Interest Rate Concerns With the rise of inflation and relatively high interest rates, companies should consider whether their disclosures regarding inflation impacts and risks as well as recent rate increases and uncertainty regarding future rate changes are adequately discussed. Depending on the effect on a company's operations and financial condition, additional disclosure of risk factors, MD&A, or the financial statements may be necessary. In recent comment letters relating to inflation, the Staff has focused on how current inflationary pressures have materially impacted a company's operations, including by pointing to statements regarding inflation made in a company's earnings materials, and sought disclosure on any mitigation efforts implemented with respect to inflation. If inflation is identified as a significant risk, the Staff asked companies to quantify, where possible, the principal factors contributing to inflationary pressures and the extent to which revenues, expenses, profits, and capital resources were impacted by inflation. In recent comment letters relating to interest rates, the Staff has asked companies to expand their discussion of rising interest rates in the Risk Factors and MD&A sections to specifically identify the actual impact of recent rate increases on the business's operations and how the business has been affected. It is also critical that companies confirm that their disclosures in "Item 7A. Quantitative and Qualitative Disclosures About Market Risk" are up-to-date and responsive to the requirements of Item 305 of Regulation S-K.

III. SEC Comment Letter Trends In 2023, comment letters from the SEC Staff continued an emphasis on addressing disclosures in management's discussion and analysis ("MD&A") as well as the use of non-GAAP measures. In addition, although the SEC's proposed climate change rules are still in flux, in 2023, the Staff continued to issue comment letters regarding companies' climate-related disclosures under the current disclosure regime, continuing the trend that started in the fall of 2021.

A. Management's Discussion and Analysis

Many of the comment letters addressing MD&A focused on disclosures relating to results of operations, with the Staff often requesting that registrants explain related disclosures with more specificity. The Staff has focused on disclosures regarding material period-to-period changes in quantitative *and* qualitative terms as prescribed by Item 303(b) of Regulation S-K. For example, the Staff has commented on disclosures about factors contributing to gross profit and revenue, to request that registrants provide both quantitative detail regarding the extent to which certain factors have impacted gross profit, as well as qualitative factors like which factors contribute to certain business sectors having a greater effect on gross product. The Staff has also requested that registrants make disclosures about known trends and uncertainties affecting their results of operations. Another area that the Staff has focused on is ensuring that key performance indicators (“KPIs”) are properly contextualized so that they are not misleading. The Staff has, in certain circumstances, requested that registrants provide additional disclosures about why KPIs are useful to investors, how they are used by management, and if there are any estimates or assumptions being used to calculate the various metrics. The Staff has also often asked registrants to quantify and provide additional disclosure regarding significant components of financial condition and results of operations that have affected segment results. Two other key areas of MD&A that the Staff focused on were critical accounting estimates and liquidity and capital resources. The Staff frequently noted that registrants’ disclosures regarding critical accounting estimates were too general, and requested that registrants provide a more robust analysis, consistent with the requirement now set forth in Item 303(b)(3) of Reg S-K. The Staff indicated that these disclosures should supplement, not duplicate, the disclosures in footnotes to financial statements.

B. Non-GAAP Financial Measures

The Staff expressed concerns regarding the improper use of non-GAAP measures in filings and issued several comments aligned with the Compliance and Disclosure Interpretations (“C&DIs”) released last December. Comments related to the latest C&DIs included a focus on whether operating expenses are “normal” or “recurring” (and therefore, whether exclusion from non-GAAP financial measures might be misleading). The Staff has also asked registrants about whether certain non-GAAP adjustments to revenue or expenses have made the adjustments “individually tailored.” In addition to a focus on the topics covered under the C&DIs, the Staff focused on a number of other matters relating to compliance with Item 10(e) of Regulation S-K, including prominence of non-GAAP measures, reconciliations, usefulness and purpose of particular measures, the exclusion of normal, recurring cash operating expenses (Non-GAAP C&DI 100.01), and the use of individually tailored accounting principles (Non-GAAP C&DI 100.04).

C. Segment Reporting

The Staff has also commented on a number of segment reporting disclosures. Examples of common comments include whether a registrant’s operating segments are properly categorized and the reasoning behind the aggregation of similar segments (and the factors used to identify different segments). Of particular note, the SEC has taken issue with registrations disclosing multiple measures of segment profit or loss in the notes to the financial statements and has indicated that registrants should not attempt to circumvent non-GAAP requirements when taking this approach.

D. Climate-Related Disclosures

As discussed in Part II.A above, climate-related disclosures continue to be a focus of the Staff. The Staff has often issued multiple rounds of letters on these types of disclosures, particularly when the initial response asserts that a category of climate-related disclosures is not material to its business (with the Staff frequently requesting the registrant to quantify the effects or costs or provide a materiality analysis).

IV. Other Reminders and Considerations A. Disclosure Controls and Procedures In light of the new cybersecurity disclosure rules and the end of the year for calendar companies, now is a good time for companies to take an opportunity to review their disclosure controls and

GIBSON DUNN

procedures, which are intended to help companies collect pertinent information for review for purposes of their public disclosure obligations. The SEC has demonstrated a willingness to bring enforcement action on disclosure controls as they relate to issues it sees as priorities, including recent hot-button topics such as cybersecurity and workplace misconduct. *SolarWinds (Cybersecurity)* In October 2023, the SEC brought charges against [SolarWinds Corporation](#), a software company, and its Chief Information Security Officer (the “CISO”) in connection with the cyberattack more commonly known as “SUNBURST,” which occurred in December 2020. Notably, this is the first time the SEC has brought a cybersecurity enforcement action against an individual. The SEC alleged that SolarWinds and the CISO made materially misleading statements and omissions about the company’s cybersecurity practices and risks in disclosures made on the company’s website and in public filings, which the SEC claims ultimately led to a drop in the company’s stock price following the subsequent disclosure of the SUNBURST cyberattack. Specifically, the complaint alleges that SolarWinds made a number of false statements relating to: (1) compliance with the National Institute of Standards and Technology (NIST) Cybersecurity Framework; (2) using a secure development lifecycle when creating software for customers; (3) having strong password protection; and (4) maintaining good access controls. The SEC’s complaint also states that SolarWinds had deficient disclosure controls, alleging that at the time the company was touting its cybersecurity practices in its public disclosures, the CISO and other employees knew that the company had serious cybersecurity deficiencies, with internal documents “describ[ing] numerous known material cybersecurity risks, control issues, and vulnerabilities.” In doing so, the company was concealing from the public known poor cybersecurity practices that were ultimately exploited during the SUNBURST cyberattack. The complaint seeks permanent injunctive relief, disgorgement of profits, civil penalties, and an officer and director bar against the CISO. The SEC’s actions in SolarWinds should be viewed in light of the new incident disclosure requirements on Form 8-K and recent prior enforcement cases ([Pearson PLC 2021](#) and [First American Financial Corporation in 2019](#)). In these recent enforcement cases, the SEC focused on the importance of carefully assessing the materiality of a cyber incident and found incidents to be material even when there was not an adverse impact on the companies’ businesses. *Activision Blizzard (Workplace Misconduct)* Early in 2023, the SEC charged [Activision Blizzard Inc.](#), a video game development and publishing company (recently acquired by Microsoft Corporation) (“Activision Blizzard”), with a failure to maintain disclosure controls. Specifically, the SEC alleged that Activision Blizzard “lacked controls and procedures designed to ensure that information related to employee complaints of workplace misconduct would be communicated to [company] disclosure personnel to allow for timely assessment on its disclosures.” The SEC’s order stated that management “lack[ed] sufficient information to understand the volume and substance of employee complaints of workplace misconduct,” and therefore “management was unable to assess related risks to the company’s business, whether material issues existed that warranted disclosure to investors, or whether the disclosures it made to investors in connection with these risks were fulsome and accurate.” Activision Blizzard agreed to a cease-and-desist order and to pay a \$35 million penalty to settle the charges. *DXC Technology (Non-GAAP Financial Measures)* In March 2023, the SEC settled charges against [DXC Technology Company](#), an IT services company, for making misleading disclosures about its non-GAAP financial performance in multiple reporting periods from 2018 until 2020. Specifically, the SEC alleged that the company materially increased its non-GAAP earnings by negligently misclassifying tens of millions of dollars of expenses as transaction, separation and integration-related (“TSI”) costs and improperly excluding these expenses as non-GAAP adjustments. The SEC noted that “[t]he absence of a non-GAAP policy and specific disclosure controls and procedures caused employees within the [company] to make subjective determinations about whether expenses were related to an actual or contemplated transaction, regardless of whether the costs were actually consistent with the description of the adjustment included in the company’s public disclosures.” The order went on to explain that the company’s controller group and disclosure committee “negligently failed to evaluate the company’s non-GAAP disclosures adequately” and even failed to recognize that for years the company did not have a non-GAAP policy and adequate disclosure controls and procedures in place. Ultimately, the company’s negligence led to misstating the nature

and scope of its TSI costs resulting in materially misleading statements. The company agreed to pay an \$8 million penalty and to undertake to develop and implement appropriate non-GAAP policies and disclosure controls and procedures. *Charter Communications Inc. (Internal Accounting Controls)* In November 2023, the SEC charged [Charter Communications Inc.](#), a telecommunications company, 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. Under Rule 10b5-1, a trading plan intended to satisfy the rule may not permit the person who entered into the plan to exercise any subsequent influence over how, when, or whether to effect transactions under the plan. According to the SEC order in *Charter Communications*, many of the company's trading plans contained "accordion" provisions allowing for increases to the amount of share repurchases if the company opted to conduct certain debt offerings. The SEC asserted that, since these debt offerings were available at the company's discretion, this feature 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, inconsistent with the board's authorization. The SEC order explained 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" and Charter ultimately paid \$25 million to settle the claims.^[22] In light of these recent enforcement actions, it is important for companies to regularly review their disclosure controls and procedures to identify and stay apprised of key risks that are relevant to the company. **B. Characterization of Legal Proceedings** Public companies often characterize legal proceedings in their securities filings as "without merit." However, companies may want to reconsider relying on this boilerplate phrase in their legal proceedings disclosures following a decision in the fall of 2023 from the United States District Court for the District of Massachusetts. In *City of Fort Lauderdale Police and Firefighters' Retirement System v. Pegasystems Inc.*,^[23] plaintiff shareholders initiated a class action against Pegasystems Inc. ("Pegasystems") after it was ordered to pay over \$2 billion in damages in a prior lawsuit regarding trade secret misappropriation. Although it did not initially disclose the trade secret matter in its securities filings when the lawsuit was first initiated in May 2020, Pegasystems eventually disclosed the matter in its Form 10-K in February 2022 stating its belief that "the claims brought against the defendants are without merit," it had "strong defenses to these claims," and "any alleged damages claimed by Appian are not supported by the necessary legal standard." Pegasystems' stock price dropped by about 16% the following day and, in May 2022, the jury returned a unanimous verdict in favor of the plaintiff in the trade secret matter. In the subsequent class action, plaintiff shareholders alleged that Pegasystems made a number of false statements and falsely reassured investors that the claims in the trade secret matter were "without merit," in light of the fact that its CEO was allegedly aware of the corporate espionage campaign. The court found that this was an actionable opinion statement explaining that "a reasonable investor could justifiably have understood [the CEO]'s message that [the trade secret] claims were 'without merit' as a denial of the facts underlying [the] claims—as opposed to a mere statement that Pega[systems] had legal defenses against those claims." The court went on to say that Pegasystems was not required to admit any wrongdoing in its disclosure and that "[a]n issuer may legitimately oppose a claim against it, even when it possesses subjective knowledge that the facts underlying the claims against it are true. When it decides to do so, however, it must do so with exceptional care, so as not to mislead investors. For example, an issuer may validly assert its intention to oppose the lawsuit. . . . It also may state that it has 'substantial defenses' against it, if it reasonably believes that to be true. . . . An issuer may not, however, 'make misleading substantive declarations regarding its beliefs about the merits of the litigation.'" The court's decision provides a cautionary tale against using boilerplate disclosure language when describing a company's litigation matters, particularly where those disclosures are contradictory to the actual prospect of an adverse result. Going forward, companies should avoid relying on boilerplate language such as "without merit" to describe claims in a lawsuit; often times, there is at least some merit to litigation even if a defendant has a strong legal defense. Instead, statements like "we intend to contest this matter vigorously" or "we have substantial defenses" (if supportable) might be appropriate alternatives. Counsel for

companies should carefully evaluate their legal proceedings disclosures—even for those matters that have previously been disclosed—and consider seeking input from management in assessing any allegations asserted against the company.

C. EDGAR Next On September 13, 2023, the SEC proposed amendments to Rules 10 and 11 of Regulation S-T and Form ID regarding potential technical changes to EDGAR filer access and account management (referred to by the SEC as “EDGAR Next”). EDGAR Next would require filers to authorize designated account administrators to manage the filers’ accounts and make filings on the filers’ behalf and would require these account administrators and any other authorized users to have their own individual account credentials to access EDGAR Next. For details on the proposed amendments, see our prior post on this topic.^[24] In connection with the proposed amendments, the SEC opened a public beta environment that is available until March 15, 2024 for filers to test and provide feedback on the technical functionality of the changes contemplated by EDGAR Next. Details regarding how to access the EDGAR Next beta environment and related resources are available at the SEC’s dedicated EDGAR Next website.^[25]

D. Filing Requirement for “Glossy” Annual Report As discussed in last year’s alert, in June 2022 the SEC adopted amendments requiring that annual reports sent to shareholders pursuant to Exchange Act Rule 14a-3(c), otherwise known as “glossy” annual reports, must also be submitted to the SEC in the electronic format in accordance with the EDGAR Filer Manual. These annual reports will be in PDF format, and filed using EDGAR Form Type ARS. In its final rule, the SEC noted that electronic submissions in PDF format of the glossy annual report should capture the graphics, styles of presentation, and prominence of disclosures (including text size, placement, color, and offset, as applicable) contained in the reports. As noted in our report last year, this may cause technical concerns with file sizes when filing through EDGAR, and companies should be mindful of the file size of their glossy annual report and conduct test runs in advance of filing.

E. Cover Page XBRL Disclosures On September 7, 2023, the SEC published a sample comment letter regarding XBRL disclosures.^[26] Contained in this sample comment letter was a comment regarding how common shares outstanding are reported on the cover page as compared to on the company’s balance sheet. The sample comment addresses instances in which companies “present the same data using different scales (presenting the whole amount in one instance and the same amount in thousands in the second).” Companies thus should consider presenting their outstanding share data consistently throughout their Form 10-K.

* * * * *

The 2023 Form 10-K will require a number of new disclosures for the first time. Companies should start drafting their disclosures earlier rather than later, particularly where disclosures will require coordination with a number of teams, such as with the new cybersecurity disclosure requirements. Looking ahead, there are several rules the SEC is expected to enact that have the potential to significantly impact future filings, including the highly anticipated climate disclosure rules, which have been pending since March 2022 and may require public companies to disclose their greenhouse gas emissions, those of their suppliers, and their downstream emissions. The latest Reg Flex agenda suggested that these rules would be finalized in October 2023, though this target has moved several times. Additionally, the Financial Accounting Standards Board (FASB) has finalized rules related to enhanced tax disclosures and segment reporting that apply starting with the 2024 10-K^{[27],[28]} and is considering rules regarding the disaggregation of expenses^[29], each of which may require a significant amount of preparation. _____^[1]

See “Announcement Regarding Share Repurchase Disclosure Modernization Rule” (Nov. 22, 2023), *available* at <https://www.sec.gov/corpfin/announcement/announcement-repurchase-disclosure-modernization-112223> ^[2] Gibson Dunn’s Securities Regulation Monitor is a blog site that provides frequent updates on securities law and corporate governance developments and is available at <https://securitiesregulationmonitor.com/default.aspx> ^[3] For a further discussion on the share repurchase requirements, please see our prior client alert “SEC Adopts Amendments to Enhance Company Stock Repurchase Disclosure Requirements” (May 5, 2023), *available* at <https://www.gibsondunn.com/sec-adopts-amendments-to-enhance-company-stock->

GIBSON DUNN

[repurchase-disclosure-requirements/](#). [4] See “SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies” (July 26, 2023), available at <https://www.sec.gov/news/press-release/2023-139>. [6] See “SEC Adopts Amendments to Modernize Rule 10b5-1 Insider Trading Plans and Related Disclosures” (Dec. 14, 2023), available at <https://www.sec.gov/news/press-release/2022-222>. [7] Available at <https://www.securitiesregulationmonitor.com/Lists/Posts/Post.aspx?ID=480>. [8] Available at <https://www.securitiesregulationmonitor.com/Lists/Posts/Post.aspx?ID=480>. [9] See “SEC Adopts Compensation Recovery Listing Standards and Disclosure Rules” (Oct. 26, 2022), available at <https://www.sec.gov/news/press-release/2022-192>. [10] Item 402 of Regulation S-K now requires companies to disclose how they have applied their recovery policies. If, during its last completed fiscal year, the company either completed a restatement that required recovery or there was an outstanding balance of excess incentive-based compensation relating to a prior restatement, the company must disclose (i) the date which the company was required to prepare each accounting restatement, the aggregate dollar amount of excess, and an analysis of how it was calculated; (ii) if the compensation is related to a stock price or TSR metric, the estimates used to determine the amount of erroneously awarded compensation; (iii) the aggregate dollar amount of excess incentive-based compensation that remained outstanding at the end of the company’s last completed fiscal year; (iv) the amount of recovery foregone under any impracticability exception used; and (v) for each current and former named executive officer, the amounts of incentive-based compensation that are subject to a clawback but remain outstanding for more than 180 days since the date the company determined the amount owed. [11] Center for Audit Quality SEC Regulations Committee Highlights, Joint Meeting with SEC Staff (June 15, 2023), available at <https://www.thecaq.org/wp-content/uploads/2023/09/June-15-2023-Joint-Meeting-HLs-FINAL-for-Posting-9-5-23.pdf> (Section III.D.). [12] For background on the CSRD, see “European Union’s Corporate Sustainability Reporting Directive—What Non-EU Companies with Operations in the EU Need to Know,” Gibson Dunn (Nov. 2022), available at <https://www.gibsondunn.com/european-union-corporate-sustainability-reporting-directive-what-non-eu-companies-with-operations-in-the-eu-need-to-know/>, and “European Corporate Sustainability Reporting Directive (CSRD): Key Takeaways from Adoption of the European Sustainability Reporting Standards,” Gibson Dunn (Aug. 2023), available at <https://www.gibsondunn.com/european-corporate-sustainability-reporting-directive-key-takeaways-from-adoption-of-european-sustainability-reporting-standards/>. For background on California’s recently enacted climate disclosure laws, see “California Passes Climate Disclosure Legislation,” Gibson Dunn (Sept. 2023), available at <https://www.gibsondunn.com/california-passes-climate-disclosure-legislation/>, and “UPDATE: California Governor Signs Climate Legislation Into Law, Bug Signals Changes to Come,” Gibson Dunn (Oct. 2023), available at <https://www.securitiesregulationmonitor.com/Lists/Posts/Post.aspx?ID=487>. [13] For more information on the SEC’s proposed rules on climate-related disclosure, see “The Enhancement and Standardization of Climate-Related Disclosures for Investors,” SEC (Apr. 2022), available at <https://www.sec.gov/files/rules/proposed/2022/33-11042.pdf>, and “Summary of and Considerations Regarding the SEC’s Proposed Rules on Climate Change Disclosure,” Gibson Dunn (Apr. 2022), available at <https://www.gibsondunn.com/summary-of-and-considerations-regarding-the-sec-proposed-rules-on-climate-change-disclosure/>. [14] For a discussion of the 2021 and 2022 comment letters, see “SEC Staff Scrutiny of Climate Change Disclosures Has Arrived: What to Expect And How to Respond,” Gibson Dunn (Sept. 2021), available at <https://www.securitiesregulationmonitor.com/Lists/Posts/Post.aspx?ID=446> and “Considerations for Preparing Your 2022 Form 10-K,” Gibson Dunn (Jan. 2023), available at <https://www.gibsondunn.com/wp-content/uploads/2023/01/considerations-for-preparing-your-2022-form-10-k.pdf>. [15] Available at <https://www.gibsondunn.com/considerations-for-climate-change-disclosures-in-sec-reports/>. [16] See “Modernization of Regulation S-K Items 101, 103, and 105, Release No. 33-10825” (Aug. 26, 2020), available at <https://www.sec.gov/rules/final/2020/33-10825.pdf>.

GIBSON DUNN

[17] Available at

<https://www.gibsondunn.com/form-10-k-human-capital-disclosures-continue-to-evolve/>.

[18] Available at

<https://www.sec.gov/files/spotlight/iac/20230921-recommendation-regarding-hcm.pdf>. [19]

See “Sample Letter to Companies Regarding Disclosures Pertaining to Russia’s Invasion of Ukraine and Related Supply Chain Issues” (May 3, 2021), available at

<https://www.sec.gov/corpfin/sample-letter-companies-pertaining-to-ukraine>. [20] Available

at

<https://www.sec.gov/corpfin/sample-letter-companies-regarding-china-specific-disclosures>.

[21] Available at

<https://www.sec.gov/corpfin/announcement/announcement-cf-pre-shutdown-communication-092723>. [22]

SEC Commissioners Hester Peirce and Mark Uyeda dissented from this decision. Commissioners Peirce and Uyeda argued that this application of the rule went too far by using Section 13(b)(2)(B)(i)’s requirement that companies “devise and maintain a system of internal accounting tools” to require that Charter Communications had sufficient systems in place to answer the legal question of whether its trading plans were in compliance with Rule 10b5-1. [23] No. CV 22-11220-WGY, 2023 WL 4706741 (D. Mass. July 24, 2023). [24] Available at

<https://securitiesregulationmonitor.com/Lists/Posts/Post.aspx?ID=483>. [25] Available at

<https://www.sec.gov/edgar/filer-information/edgar-next>. [26] Available at

<https://www.sec.gov/corpfin/sample-letter-companies-regarding-their-xbrl-disclosures>. [27]

Available at

[https://www.fasb.org/Page/ProjectPage?metadata=fasb-](https://www.fasb.org/Page/ProjectPage?metadata=fasb-Targeted%20Improvements%20to%20Income%20Tax%20Disclosures)

[Targeted%20Improvements%20to%20Income%20Tax%20Disclosures](https://www.fasb.org/page/getarticle?uid=fasb_Media_Advisory_11-27-23) [28] Available at

https://www.fasb.org/page/getarticle?uid=fasb_Media_Advisory_11-27-23. [29] Available

at

<https://www.fasb.org/Page/ShowPdf?path=Proposed+ASU%E2%80%94Income+Statement%E2%80%94Reporting+Comprehensive+Income%E2%80%94Expense+Disaggregation+Disclosures+%28Subtopic+220-40%29%E2%80%94Disaggregation+of+Income+Statement+Expenses.pdf&iitle=Proposed+Accounting+Standards+Update%E2%80%94Income+Statement%E2%80%94Reporting+Comprehensive+Income%E2%80%94Expense+Disaggregation+Disclosures+%28Subtopic+220-40%29%E2%80%94Disaggregation+of+Income+Statement+Expenses&acceptedDisclaimer=true&IsIQS=false&Submit>.

The following Gibson Dunn attorneys assisted in preparing this update: Ron Mueller, Elizabeth Ising, Mike Scanlon, Mike Titera, Julia Lapitskaya, Matthew Dolloff, David Korvin, Meghan Sherley, Victor Twu, Maggie Valachovic, and Nathan Marak.

Gibson Dunn’s lawyers are available to assist with any questions you may have regarding these developments. To learn more about these issues, please contact the Gibson Dunn lawyer with whom you usually work in the firm’s Securities Regulation and Corporate Governance or Capital Markets practice groups, or any of the following practice leaders and members: **Securities Regulation and Corporate Governance:** Elizabeth Ising – Co-Chair, Washington, D.C. (+1 202.955.8287, eising@gibsondunn.com) James J. Moloney – Co-Chair, Orange County (+1 949.451.4343, jmoloney@gibsondunn.com) Lori Zyskowski – Co-Chair, New York (+1 212.351.2309, lzyskowski@gibsondunn.com) Brian J. Lane – Washington, D.C. (+1 202.887.3646, blane@gibsondunn.com) Ronald O. Mueller – Washington, D.C. (+1 202.955.8671, rmueller@gibsondunn.com) Thomas J. Kim – Washington, D.C. (+1 202.887.3550, tkim@gibsondunn.com) Michael A. Titera – Orange County (+1 949.451.4365, mtitera@gibsondunn.com) Aaron Briggs – San Francisco (+1 415.393.8297, abriggs@gibsondunn.com) Julia Lapitskaya – New York (+1 212.351.2354, jlapitskaya@gibsondunn.com) **Capital Markets:** Andrew L. Fabens – New York, NY (+1 212.351.4034, afabens@gibsondunn.com) Hillary H. Holmes – Houston, TX (+1 346.718.6602, hholmes@gibsondunn.com) Stewart L. McDowell – San Francisco, CA (+1 415.393.8322, smcdowell@gibsondunn.com) Peter W. Wardle – Los Angeles, CA (+1 213.229.7242, pwardle@gibsondunn.com) © 2023 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. Attorney Advertising: These materials were prepared for general informational purposes only based on information available at the time of publication and

GIBSON DUNN

are not intended as, do not constitute, and should not be relied upon as, legal advice or a legal opinion on any specific facts or circumstances. Gibson Dunn (and its affiliates, attorneys, and employees) shall not have any liability in connection with any use of these materials. The sharing of these materials does not establish an attorney-client relationship with the recipient and should not be relied upon as an alternative for advice from qualified counsel. Please note that facts and circumstances may vary, and prior results do not guarantee a similar outcome.

Related Capabilities

[Securities Regulation and Corporate Governance](#)

[Capital Markets](#)

[Environmental, Social, and Governance \(ESG\)](#)

SEC Successfully Prosecutes Novel “Shadow Trading” Theory at Trial

Client Alert | April 10, 2024

The government successfully argued that trading in the securities of one company based upon material nonpublic information about a separate company (in whose securities the defendant does not trade) can nevertheless violate the federal securities laws. On April 5, 2024, a civil jury found a former biopharmaceutical executive liable for insider trading under a novel theory with potentially far-reaching implications for the government’s enforcement of Section 10(b) of the Securities Exchange Act of 1934 and Rule 10b-5 thereunder, as well as potential criminal insider trading prosecutions. In a first-of-its-kind trial, in *SEC v. Panuwat*, the government successfully argued that trading in the securities of one company based upon material nonpublic information about a separate company (in whose securities the defendant does not trade) can nevertheless violate the federal securities laws. This is called “shadow trading.” Although the SEC has been at pains to claim that there is “nothing novel” about the “pure and simple” insider trading theory it advanced in *Panuwat*,^[1] the ruling heralds a significant new application of the federal government’s insider trading authority to prevent such “shadow trading” in which corporate insiders allegedly exploit information about their own companies to profit by trading in the securities of “economically-linked firms.”^[2] **Factual Background** Matthew Panuwat served as Senior Director of Business Development at Medivation Inc., a publicly traded biopharmaceutical company specializing in oncology drugs. At the outset of his employment, Mr. Panuwat signed the company’s insider trading policy. That policy provided that he would not “gain personal benefit” by using Medivation’s information to “profit financially by buying or selling” either Medivation’s securities “or the securities of another publicly traded company.”^[3] Not all public companies prohibit their personnel (including members of the Board of Directors) from trading in the securities of other public companies or competitors. Medivation did. As alleged by the government, on August 18, 2016, Mr. Panuwat and other senior employees received an email from David Hung, Medivation’s chief executive officer, suggesting that a deal was imminent in which Medivation would be purchased by Pfizer. Although market participants already knew that Medivation had been fielding offers for several months, the SEC alleged that Hung’s email contained several pieces of non-public information. Mr. Panuwat, who had been part of the Medivation deal team, knew that the bids from potential acquirers including Pfizer represented a substantial premium over the then-existing market price for Medivation shares. Seven minutes after receiving Mr. Hung’s email, Mr. Panuwat began purchasing call options for Incyte Corporation, one of a handful of similar publicly traded biopharmaceutical companies focused on late-stage oncology treatments. When Pfizer’s acquisition of Medivation was publicly announced a few days later, Incyte’s stock increased 7.7% and Mr. Panuwat made approximately \$110,000 from his call options. On August 17, 2021, the SEC brought an action against Mr. Panuwat for insider trading under Section 10(b) of the Exchange Act, alleging a single violation of Rule 10b-5. **The District Court Denied Mr. Panuwat’s Motion to Dismiss** Mr. Panuwat moved to dismiss the SEC’s complaint on multiple grounds, including that the SEC’s unprecedented “shadow trading” theory sought to hold him liable for trading in Incyte’s securities as a result of his knowledge of the Pfizer-Medivation acquisition violated his constitutional right to Due Process. Mr. Panuwat argued that such a theory had never before been advanced in litigation. According to this line of argument, market participants had not previously understood that “confidential information regarding an acquisition involving Company A should also be considered material to Company B (and presumably companies C, D, E, etc.) that operate within the same general industry.”^[4] Although the Court agreed that

Related People

[Reed Brodsky](#)

[Benjamin Wagner](#)

[Mark K. Schonfeld](#)

[David Woodcock](#)

[Ronald O. Mueller](#)

[Lori Zyskowski](#)

[Thomas J. Kim](#)

[Julia Lapitskaya](#)

[Michael L. Nadler](#)

[Edmund Bannister](#)

there “appear to be no other cases” supporting that proposition, and the SEC “conceded this at oral argument,” the Court nevertheless rejected this Due Process argument. The Court held that the SEC’s theory fell “within the general framework of insider trading, and the expansive language” of federal securities laws.^[5] The lengthiest portion of the Court’s decision, as well as the parties’ briefing, concerned whether information regarding the Pfizer-Medivation acquisition was material to Incyte. Mr. Panuwat argued that the information he received was not “about” Incyte, a non-party to the imminent transaction.^[6] But the Court concluded that “given the limited number of mid-cap, oncology-focused biopharmaceutical companies with commercial-stage drugs in 2016, the acquisition of one such company (Medivation) would make the others (*i.e.*, Incyte) more attractive, which could then drive up their stock price.” The Court stated that it was “reasonable to infer” that other companies that had unsuccessfully attempted to acquire Medivation “would turn their attention to Incyte” after losing out to Pfizer.^[7] And, more broadly, in *dicta* the Court endorsed the SEC’s “common-sense” argument that “information regarding business decisions by a supplier, a purchaser, or a peer can have an impact on a company” and therefore be material—a potentially far-reaching endorsement of the SEC’s novel “shadow trading” theory.^[8] In addition, the parties agreed that Mr. Panuwat owed a duty to Medivation in light of his role as a senior executive of the company. That supported the SEC’s theory that he could be liable for misappropriating Medivation’s material non-public information concerning its impending acquisition. Although Mr. Panuwat argued that trading Incyte securities did not violate his duties to Medivation, the Court disagreed. At the pleading stage, the Court relied on “the plain language” of Medivation’s insider trading policy prohibiting trading “the securities of another publicly traded company, including . . . competitors” of Medivation, which could be read to include Incyte.^[9] The Court further found that *scienter* could be reasonably inferred given that Mr. Punawat allegedly traded the Incyte call options “within minutes” of receiving Mr. Hung’s email but had “never traded Incyte stock before.”^[10]

A Jury Agrees Mr. Panuwat’s Trading Falls Within the SEC’s “Shadow Trading” Theory In November 2023, the Court denied Mr. Panuwat’s motion for summary judgment. The Court found that a key question for the jury was whether the SEC could prove “a connection between Medivation and Incyte” such that “a reasonable investor would view the information in the Hung Email as altering the ‘total mix’ of information available about Incyte.”^[11] In particular, the Court recognized at least three ways in which the SEC might be able to prevail on this question of fact. First, it recognized that the SEC had introduced several “analyst reports and financial news articles” that “repeatedly linked Medivation’s acquisition to Incyte’s future.”^[12] Mr. Panuwat tried to sever this link by arguing that Medivation and Incyte did not consider themselves competitors because they offered somewhat different products. The Court, however, rejected this argument because “no legal authority suggest[ed] that a reasonable investor would conclude that Medivation’s acquisition would only affect the stock price of companies that directly competed” with it.^[13] Second, the SEC introduced evidence that “Medivation’s investment bankers considered Incyte a ‘comparable peer’” for valuation purposes because both were mid-cap biopharmaceutical companies with cancer-related drugs.^[14] Third, the Court found that Incyte’s stock price increased by 7.7% after announcement of the Pfizer-Medivation acquisition, which the Court inferred was itself “strong evidence” investors understood “the significance of that information” as being material to Incyte.^[15]

SEC v. Panuwat proceeded to an eight-day jury trial that began on March 25, 2024. After only about two hours of deliberation, on April 5, the jury returned a verdict finding that Mr. Panuwat’s purchase of Incyte call options constituted insider trading in violation of Section 10(b) of the Securities Exchange Act of 1934 and Rule 10b-5 promulgated thereunder. That same day the SEC issued a press release noting that the brevity of the jury’s deliberations supported the SEC’s position since the outset of the litigation, quoting Division of Enforcement Director Gurbir S. Grewal as saying that, “As we’ve said all along, there was nothing novel about this matter, and the jury agreed: this was insider trading, pure and simple” because Mr. Panuwat “used highly confidential information about an impending announcement” of Medivation’s acquisition “to trade ahead of the news for his own enrichment” by using “his employer’s confidential information to acquire a large stake in call options” of Incyte, which “increased materially on the important news.”^[16]

Depending on the Appellate Court, “Shadow Trading” Liability May Be Here to Stay

Pending the results of the anticipated appeal, the successful prosecution of Mr. Panuwat has armed the federal government with a powerful new precedent. Academic studies have claimed to find “robust evidence” that “shadow trading” is a frequent real-world phenomena in which “employees circumvent insider trading regulations” by “trading in their firm’s business partners and competitors” rather than trading in their own employers’ securities.^[17] The district court’s detailed rulings in *SEC v. Panuwat* provide a clear blueprint for the government’s approach moving forward. Further, the jury’s findings against Mr. Panuwat after deliberating for only a few hours provides anecdotal evidence that litigating “shadow trading” cases is a viable option for government regulators and prosecutors. Depending on whether Mr. Panuwat appeals the decision (as expected), legal and compliance professionals would be well-advised to continue to keep “shadow trading” issues in mind when designing, revising and implementing their firms’ trading policies and training programs. Indeed, anyone who trades in securities while in possession of material non-public information—including corporate insiders and directors, bankers, accountants, and lawyers, among others—could find themselves within the zone of a “shadow trading” theory. In addition, commencing with annual reports on Forms 10-K for fiscal years beginning on or after April 1, 2023, public companies will need to file as an exhibit to their Form 10-Ks any “insider trading policies and procedures governing the purchase, sale, and/or other dispositions of the registrant’s securities” that “are reasonably designed to promote compliance with insider trading laws, rules and regulations.”^[18] While this requirement does not literally apply to policies addressing the trading of other companies’ securities, some companies have policies (as with Medivation) that address such trading.^[19] Companies should carefully consider all factors in deciding whether to prohibit trading in other securities, and conduct training of insiders and board members as to the SEC’s expansive views on the scope of the law against insider trading. Moreover, the securities laws impose obligations on SEC-registered firms, namely investment advisers and broker-dealers, to adopt and implement policies and procedures reasonably designed to prevent the misuse of material nonpublic information. Such firms can often be confronted with questions as to the scope of a restriction imposed by the receipt of material nonpublic information subject to a duty of confidentiality, while simultaneously fulfilling fiduciary duties to manage assets in the interests of clients. Such questions can arise at the inception of a trading restriction as well as at later points during the period of restriction. Judgments about the materiality of information about one company to the price of securities of another company are particularly nuanced and complicated. For example, it can be difficult to determine whether favorable news about one company will have a positive or negative impact on a competitor. Hanging over all of this is the ever-present risk that the SEC views the facts with the benefit of hindsight. Legal and compliance functions at investment advisers and broker-dealers may wish to revisit their policies and procedures in light of the shadow trading risk, as well as train their investment professionals to be sensitized to the risks the case highlights. As always, Gibson Dunn remains available to help its clients in addressing these issues. ^[1] SEC, *Statement on Jury’s Verdict in Trial of Matthew Panuwat*, Apr. 5, 2024 <https://www.sec.gov/news/statement/grewal-statement-040524>. ^[2] Mihir Mehta, David Reeb, & Wanli Zhao, *Shadow Trading* 1, Accounting Review (July 2021), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3689154. ^[3] Complaint ¶ 20, *SEC v. Panuwat*, No. 21-cv-06322 (N.D. Cal. Aug. 17, 2021) ^[4] *SEC v. Panuwat*, 2022 WL 633306, at *8 (N.D. Cal. Jan. 14, 2022). ^[5] *Id.* ^[6] *Id.* at *4. ^[7] *Id.* at *5. ^[8] *Id.* at *4. ^[9] *Id.* at *6. ^[10] *Id.* at *7. ^[11] *SEC v. Panuwat*, 2023 WL 9375861, at *5 (N.D. Cal. Nov. 20, 2023). ^[12] *Id.* at *6. ^[13] *Id.* ^[14] *Id.* ^[15] *Id.* ^[16] SEC, *Statement on Jury’s Verdict in Trial of Matthew Panuwat*, Apr. 5, 2024 <https://www.sec.gov/news/statement/grewal-statement-040524>. ^[17] Mihir Mehta, David Reeb, & Wanli Zhao, *Shadow Trading* 1, 4, Accounting Review (July 2021), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3689154. ^[18] Item 408(b) of Regulation S-K (emphasis added). Smaller reporting companies have to comply with the requirements beginning with their Form 10-K for fiscal years beginning on or after October 1, 2023. ^[19] Under Section 21A(b)(1) of the Exchange Act, public companies are not subject to controlling person liability for insider trading by executives, directors, or employees unless they disregarded the fact that a controlled person was likely to engage in the act or acts constituting the violation and failed to take appropriate steps to prevent

GIBSON DUNN

such act or acts before they occurred.

The following Gibson Dunn lawyers assisted in preparing this update: Reed Brodsky, Benjamin Wagner, Mark Schonfeld, David Woodcock, Ronald Mueller, Lori Zyskowski, Thomas Kim, Julia Lapitskaya, Michael Nadler, Edmund Bannister, and Peter Jacobs*.

Gibson, Dunn & Crutcher's lawyers are available to assist in addressing any questions you may have regarding these issues. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any leader or member of the firm's Securities Enforcement or Securities Regulation and Corporate Governance practice groups:

Securities Enforcement: Reed Brodsky – New York (+1 212.351.5334, rbrodsky@gibsondunn.com) Mark K. Schonfeld – New York (+1 212.351.2433, mschonfeld@gibsondunn.com) Benjamin Wagner – Palo Alto (+1 650.849.5395, bwagner@gibsondunn.com) David Woodcock – Dallas/Washington, D.C. (+1 214.698.3211, dwoodcock@gibsondunn.com) Michael Nadler – New York (+1 212.351.2306, mnadler@gibsondunn.com) **Securities Regulation and Corporate Governance:** Elizabeth Ising – Washington, D.C. (+1 202.955.8287, eising@gibsondunn.com) Thomas J. Kim – Washington, D.C. (+1 202.887.3550, tkim@gibsondunn.com) Julia Lapitskaya – New York (+1 212.351.2354, jlapitskaya@gibsondunn.com) James J. Moloney – Orange County (+1 1149.451.4343, jmoloney@gibsondunn.com) Ronald O. Mueller – Washington, D.C. (+1 202.955.8671, rmueller@gibsondunn.com) Lori Zyskowski – New York (+1 212.351.2309, lzyskowski@gibsondunn.com) *Peter Jacobs is an associate working in the firm's New York office who is not yet admitted to practice law. © 2024 Gibson, Dunn & Crutcher LLP.

All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. Attorney Advertising: These materials were prepared for general informational purposes only based on information available at the time of publication and are not intended as, do not constitute, and should not be relied upon as, legal advice or a legal opinion on any specific facts or circumstances. Gibson Dunn (and its affiliates, attorneys, and employees) shall not have any liability in connection with any use of these materials. The sharing of these materials does not establish an attorney-client relationship with the recipient and should not be relied upon as an alternative for advice from qualified counsel. Please note that facts and circumstances may vary, and prior results do not guarantee a similar outcome.

Related Capabilities

[Securities Enforcement](#)

[Securities Regulation and Corporate Governance](#)

SEC UPDATE

2024 YEAR-TO-DATE

Mark Schonfeld, David Woodcock, Tina Samanta

GIBSON DUNN

MCLE CERTIFICATE INFORMATION

MCLE Certificate Information

- Approved for 1.0 hour General PP credit.
- CLE credit form must be submitted by **Thursday, October 31st**.
- Form Link: https://gibsondunn.qualtrics.com/jfe/form/SV_6wWtTliqzBZYvAO
 - Most participants should anticipate receiving their certificate of attendance in four to eight weeks following the webcast.
- **Please direct all questions regarding MCLE to CLE@gibsondunn.com.**

AGENDA

01 Overview

02 Impact of Significant Litigation

03 Notable Enforcement Sweeps

04 Financial Reporting, Disclosure, and Accounting

05 Insider Trading

06 Cooperation and Self-Reporting Credit

Overview



U.S. Securities and Exchange Commission

- **Key Leadership Changes in 2024**
- **Impact of the Election on SEC Rulemaking and Enforcement**
- **Reflections on the Commission Under Gensler**

SEC Leadership Changes in 2024

SEC Division of Enforcement has a new leader as of October 11, 2024, which could have implications for the direction of the agency.

- **Gurbir S. Grewal**, Director of the Division of Enforcement who led the SEC's crackdown on cryptocurrency industry and Wall Street's use of off-channel communications, stepped down effective **October 11, 2024**.
- **Sanjay Wadhwa**, who has been with the SEC for more than two decades, was named as **Acting Director**.



Gurbir S. Grewal

"We have been incredibly fortunate that such an accomplished public servant, Gurbir Grewal, came to the SEC to lead the Division of Enforcement for the last three years...Every day, he has thought about how to best protect investors and help ensure market participants comply with our time-tested securities laws. He has led a Division that has acted without fear or favor, following the facts and the law wherever they may lead. I greatly enjoyed working with him and wish him well."

- SEC Chair Gensler

The Gensler Commission: Key Takeaways

Under Gary Gensler's leadership, the SEC has pursued an aggressive agenda touching on all corners of the U.S. securities markets, including:

- robust rulemaking agenda, including on market structure, climate policy, and private funds
- an active and aggressive enforcement program, with a continued focus on high-impact cases and large penalties
- focus on expanding SEC regulatory authority to address the role of crypto assets and AI in the capital markets



Impact of Significant Litigation on the Commission

Key Litigation Updates:

Overview

There have been several notable recent cases that potentially limit the scope of the SEC's enforcement authority in consequential ways.

- ***SEC v. Jarkesy* (SCOTUS) (June 2024)**
- ***SEC v. SolarWinds Corp.* (SDNY) (July 2024)**
- ***SEC v. Govil* (2d Cir.) (November 2023)**
- ***National Association of Private Funds Managers v. SEC* (5th Cir.) (June 2024)**

SEC v. Jarkesy et al.

U.S. Supreme Court

On June 27, 2024, the U.S. Supreme Court ruled that **when the SEC seeks civil penalties** against a defendant for securities fraud, the **Seventh Amendment entitles the defendant to a jury trial** before an Article III court.

The Supreme Court concluded:

- The SEC’s antifraud provisions “replicate common law fraud,” thereby requiring that a jury hear such claims.
- The public rights exception to a defendant’s jury trial right did not apply to SEC antifraud claims because such claims did not fall within “any of the distinctive areas involving governmental prerogatives where the Supreme Court has previously concluded that a matter may be resolved outside of an Article III Court, without a jury.”

On July 18, 2024, the District Court for the SDNY **dismissed many of the SEC's claims** against the company and its former CISO relating to the Company's disclosures, but did sustain claim alleging that a website "Security Statement" in 2017 was misleading. Notable points include:

- Alleged cybersecurity deficiencies are not actionable under internal accounting and disclosure controls rules
- Isolated disclosure failures do not equate to inadequate disclosure controls and procedures
- Statements concerning the incident in press releases, blog posts and podcasts were "too general to cause a reasonable investor to rely upon them"
- The incident did not require amendment of risk disclosures that already warned investors of risks "in sobering terms."
- Omission of details of incident was not misleading where the disclosure, "read as a whole, captured the big picture"

SEC v. SolarWinds Corp. and T. Brown

S.D.N.Y.

SEC v. Govil

2d Circuit

In November 2023, the Court of Appeals for the Second Circuit held that the SEC is **not entitled to disgorgement unless it can show that the allegedly defrauded investors suffered pecuniary harm**, reversing a disgorgement judgment against an executive who misappropriated funds from his company.

The Court followed the Supreme Court's decision in *Liu v. SEC* and concluded:

- Liu “emphasized” that disgorgement as “an equitable remedy is about ‘returning the funds to victims,’” which necessarily “presupposes pecuniary harm” as funds “cannot be returned if there was no deprivation in the first place.”
- The decision potentially puts in question the SEC’s ability to seek disgorgement in a wide range of enforcement actions in the absence identifiable victims who incurred a financial loss.

National Association of Private Fund Managers v. SEC

5th Circuit

On June 5, 2024, the Fifth Circuit **vacated in full the SEC’s 2023 final rule to enhance the regulation of private fund advisers** (the “Private Funds Rule”), which imposed substantial new disclosure requirements and restricted a broad range of activities within the private funds industry.

The Court ruled that the SEC **exceeded its statutory authority** under Sections 211(h) and 206(4) of the Advisers Act in adopting the Private Funds Rule.

Importantly, in reaching its decision the Fifth Circuit held that the SEC’s authority under Section 211(h) is **limited to “retail investors”** and that to promulgate rules under Section 206(4) the SEC is required to articulate a “rational connection” to fraud and explain how such rules are designed to prevent fraud.

Notable Enforcement Sweeps

The SEC has continued its **aggressive, years-long sweep** of off-channel recordkeeping violations. There are now **more than 100 individuals and entities charged** as part of this ongoing sweep, with total **penalties of over \$3 billion** to date. Recent actions in the last 6 months include:

- In April 2024, the SEC announced settled charges against a registered investment adviser for alleged recordkeeping and ethics code violations.
- In August 2024, the SEC announced settled charges **against twenty-six** broker-dealers, investment advisers, and dually-registered broker-dealers and investment advisers.
- In September 2024, the SEC announced **four rounds** of settled charges against credit ratings agencies, municipal advisors, broker-dealers, and investment advisers.

NOTE: The firms that self-reported their violations paid significantly less in penalties.

Recordkeeping Sweep

Whistleblower Protection Sweep

- On September 9, 2024, the SEC announced settled enforcement actions against seven companies for violating the SEC's whistleblower protection rule, alleging that the companies had provisions in various kinds of agreements with employees, including employment, separation, and settlement agreements, that **purport to restrict, and thereby could potentially discourage, employees and other signatories from reporting information to government investigators** or participating in a whistleblower award.
- In its sweep, the SEC included companies from various industries, including fashion, healthcare, software, manufacturing, and consumer credit reporting. Penalties ranged from \$19,500 (against a company with a going concern opinion and \$8,890 in cash) to \$1,386,000 and totaled **more than \$3 million**.

NOTE: The SEC assessed penalties notwithstanding the companies' remedial efforts once approached by the SEC and the fact that the provisions had never been invoked to prevent a party from making a claim or seeking compensation as a whistleblower.

Section 16 Reporting Sweep

- On September 25, 2024, the SEC announced a sweep of enforcement actions against twenty-three entities and individuals for **failing to timely file reports on their holdings and transactions** in violation of Section 13 and Section 16 of the Securities Exchange Act of 1934 (Exchange Act).
- Additionally, two public companies settled claims for contributing to their officers' and directors' filing failures and for not disclosing their insiders' filing delinquencies as required by SEC rules.
- The penalties ranged from \$10,000 to \$200,000 for individuals and \$40,000 to \$750,000 for public companies.
- This sweep is **part of an ongoing enforcement initiative**, launched in 2014, that focuses on these reporting requirements and particularly on the habitual late filers.
- The latest sweep is **one of the largest to date** in terms of the number of individuals and entities.

NOTE: In announcing the settlements, the SEC once again highlighted its use of data analytics to identify individuals and entities who filed late reports.

Marketing Rule Sweep

- On September 9, 2024, the SEC settled charges against **nine registered investment advisers** for violations of Rule 206(4)-1 (the “Marketing Rule”) by **disseminating advertisements that included untrue or unsubstantiated statements** of material fact or testimonials, endorsements, or third-party ratings that lacked required disclosures.
- The alleged violations were found primarily on the Advisers’ **public websites** and, in one instance, third-party public websites and social media sites, among other marketing materials.
- The advisers ranged in size from \$191 million to \$5.2 billion in regulatory assets under management and paid civil monetary penalties ranging from \$60,000 to \$325,000.
- The 2024 sweep follows a **similar enforcement sweep in 2023**, which involved nine investment advisers and a total of \$850,000 in combined penalties.

Financial Reporting, Disclosure, and Accounting Developments

S.D.N.Y. Motion to Dismiss SolarWinds Decision

Internal Accounting Controls

- The court found that the SEC’s attempt to bring a claim under Section 13(b)(2)(B) of the Exchange Act (relating to internal accounting controls) was **unsupported by legislative intent**, as the surrounding terms that Congress used when drafting Section 13(b)(2)(B), which refer to “transactions,” “preparation of financial statements,” “generally accepted accounting principles,” and “books and records,” are uniformly consistent with financial accounting.

Disclosure Controls and Procedures

- The court sided with SolarWinds in rejecting the SEC’s claims that the company failed to maintain and adhere to appropriate disclosure controls for cybersecurity incidents. The court was unwilling to accept the SEC’s argument that one-off issues—even if the company misapplied its existing disclosure controls in considering cybersecurity incidents—gave rise to a claim that the company failed to maintain such controls. The court implied that **disclosure controls do not have to be perfect**—they should provide reasonable assurance that information is being collected for disclosure consideration.

Dissenting statements on enforcement actions by Commissioners, most notably Commissioner Peirce, are becoming increasingly more common, especially with respect to the **expansion of the SEC's interpretation of its enforcement authority** under Section 13(B)(2)(b) (internal controls).

E.g. Statement on R.R. Donnelley & Sons, Co. (July 2024): “Identifying a link between the Commission’s preferred policies and procedures and accounting controls seems a collateral concern, if it is a concern at all. In today’s settled administrative proceeding against R.R. Donnelly & Sons, Co., the Commission finds and uses a novel attachment on its multi-use tool—’a system of cybersecurity-related internal accounting controls.’”

Commissioner Dissents

Voluntary Dismissal of 102(e) Proceedings

- Following the Supreme Court's *Jarkesy* decision, the SEC **voluntarily dismissed multiple 102(e) proceedings** against accountants who had been sued in administrative proceedings for allegedly faulty audits.
- This suggests the SEC had **concerns about the constitutionality** of these proceedings.
- Future enforcement uncertain.

Notable Insider Trading Developments

“Shadow Insider Trading”: Panuwat

- SEC charged Panuwat, a business development executive at Medivation, with insider trading.
- Within minutes of learning Medivation would be acquired by Pfizer at a premium, Panuwat bought short-term out-of-the-money call options in Incyte, a competitor of Medivation, which he anticipated would increase in price when the Medivation deal became public.
- Medivation’s insider trading policy prohibited the use of MNPI to trade in securities of Medivation or “another publicly traded company”
- When the Medivation deal was announced, Incyte stock increased 8%
- Court **denied defense motion to dismiss**, as “the SEC’s theory of liability falls within the general framework of insider trading”
- After 2 hours’ deliberation, **jury found Panuwat liable** for insider trading.

Credit Markets:

Sound Point Capital

- SPC managed CLOs and traded the tranches of CLOs both that it managed and that were managed by third parties.
- SPC **lacked written policies and procedures** aimed at preventing the misuse of MNPI about the underlying loans when trading tranches of CLOs.
- In 2019, SPC sold equity tranches of two CLOs it managed and that included loans to Company A. Before the sale, SPC had received MNPI about Company A through participation in an ad hoc lender committee for Company A.
- MNPI concerned likely failure of an asset sale and need for rescue financing.
- When the MNPI became public the next day, the value of the CLO tranches declined 50%. One of the buyers of the CLOs demanded reimbursement and threatened litigation. SPC agreed to reimburse.
- SEC settlement included **\$1.8 million penalty**.

Ad Hoc Committees:

Marathon Asset Management

- Marathon joined, and served on coordinating group of, ad hoc committee of creditors of Issuer. Committee retained Adviser.
- October 2020, Adviser entered into NDA with Issuer and received MNPI. Adviser conferred with committee orally and in writing. Written material were based on “publicly available” information. Marathon continued building a position in Issuer bonds and selling CDS.
- November 2020, Marathon entered into NDA with Issuer to negotiate potential restructuring. Marathon received materials from the Adviser that included “Private” or “Restricted” information.
- According to SEC’s order, Marathon’s **policies and procedures did not sufficiently take into account the special circumstances** presented by participation in committees, which included the retention of, and consultation with, financial advisers who had access to MNPI.
- Marathon had no policies or procedures for conducting due diligence on advisers’ handling of MNPI or for obtaining representations from advisers concerning policies and procedures for handling MNPI.

Credit for Cooperation and Self-Reporting

**Former
Enforcement
Director
Gurbir S.
Grewal's
Comments**

May 2024

Director Grewal stated that there are “**real benefits**” to parties that effectively cooperate with SEC investigations, which may include the SEC:

- **Charges** – recommending reduced charges or declining to recommend any charges altogether.
- **Remedies** – recommending reduced or even zero civil penalties, and effective remediation efforts may impact whether the SEC recommends any undertakings (and the scope of any such undertakings).
- **SEC Finding of Cooperation** – stating in the SEC’s order that the party provided meaningful cooperation.

Former Enforcement Director Gurbir S. Grewal's Comments

May 2024

Director Grewal also outlined “**five principles of effective cooperation**”:

- **Self-policing** – “showing that you had appropriate safeguards in place can also be important in establishing that any misconduct was not the result of an institutional failure or a lax tone at the top”
- **Self-reporting without delay** – signals “effective self-policing,” “proactive compliance,” and builds credibility with the staff
- **Remediation** – measures include disciplining or dismissing the actors responsible for the violations; strengthening relevant internal controls; conducting training; hiring personnel with relevant expertise; clawing back executive compensation; and repaying harmed investors
- **Going beyond what is legally required** – “more than simply complying with subpoenas without undue delay or gamesmanship”
- **Collaboration** – *new element* described as *effective communication with the SEC*

Strategic Considerations When Self-Reporting

There are a **range of potential outcomes to consider** when assessing whether to self-report a potential violation.

Recent examples include:

- (1) September 2023 recordkeeping sweep - unreported violations resulted in penalties between \$8 million and \$35 million, whereas self-reported violation only received penalty of \$2.5 million.
- (2) September 2024 recordkeeping sweep – unreported violations resulted in penalties between \$325,000 and \$35 million, whereas self-reported violation did not result in any penalty.

Cooperation Summary

- Seaboard factors have aged well
- Self-reporting decisions are never easy
- Whistleblowers raise the stakes
- Collaboration is hard to define
- Benefits of cooperation are hard to estimate or quantify
- Benefits of cooperation may not be known until the very end

Upcoming Programs – Fall White Collar Webcast Series

Date and Time	Program	Registration Link
<p>Thursday, November 7, 2024 1:00 PM – 2:30 PM ET 10:00 AM – 11:30 AM PT</p>	<p>False Claims Act Enforcement in the Life Sciences and Health Care Sectors Presenters: John Partridge, Jonathan Phillips, Katlin McKelvie, Jim Zelenay</p>	<p>Event Details</p>
<p>Wednesday, November 13, 2024 3:00 PM – 4:00 PM ET 12:00 PM – 1:00 PM PT</p>	<p>Government Investigations into AI Systems Presenters: Eric Vandeveld, Chris Whittaker, Poonam Kumar</p>	<p>Event Details</p>
<p>Thursday, November 14, 2024 12:00 PM – 1:00 PM ET 9:00 AM – 10:00 AM PT</p>	<p>Criminal Antitrust Enforcement: A Preview of Priorities for the New Administration and Implications for Corporate Compliance Programs Presenters: Scott Hammond, Jeremy Robison, Alexandra Buettner</p>	<p>Event Details</p>
<p>Thursday, November 21, 2024 11:00 AM – 12:00 PM ET 8:00 AM – 9:00 AM PT 4:00 PM – 5:00 PM BST</p>	<p>Investigations: A UK Perspective Presenters: Allan Neil, Matthew Nunan, Amy Cooke, Marija Brackovic</p>	<p>Event Details</p>

GIBSON DUNN

Attorney Advertising: These materials were prepared for general informational purposes only based on information available at the time of publication and are not intended as, do not constitute, and should not be relied upon as, legal advice or a legal opinion on any specific facts or circumstances. Gibson Dunn (and its affiliates, attorneys, and employees) shall not have any liability in connection with any use of these materials. The sharing of these materials does not establish an attorney-client relationship with the recipient and should not be relied upon as an alternative for advice from qualified counsel. Please note that facts and circumstances may vary, and prior results do not guarantee a similar outcome.

GIBSON DUNN



Securities Enforcement Update

August 22, 2024

Securities Enforcement 2024 Mid-Year Update

A dichotomy in enforcement: a continued aggressive enforcement agenda tempered by litigation setbacks.

I. INTRODUCTION

The first half of 2024 reflected a dichotomy in SEC enforcement. On one hand, the Enforcement Division continued to pursue an aggressive enforcement agenda, including a number of notable enforcement actions, and continued demand for heightened penalties. On the other hand, the Commission incurred a number of significant litigation setbacks with potentially broad implications for the SEC's enforcement program.

A. Notable Enforcement Activity

In the first half of 2024, the SEC won a significant insider trading litigation and continued to recover unprecedented penalties as part of its sweep activities relating to recordkeeping and whistleblower protections rules.

Shadow Trading Victory

In April 2024, the SEC won its trial against Matthew Panuwat, in a highly publicized insider trading case relating to a novel “shadow trading” theory. The SEC alleged that Panuwat's trading in a competitor company (Incyte)—which was critically *not* the subject of the inside information that he received concerning the proposed acquisition of his company (Medivation)—constituted trading on the basis of material non-public information. In denying Panuwat's motion for

summary judgment, the Court held that a jury could find that information concerning Medivation was material to Incyte on the basis that Incyte had a “market connection” to Medivation. The Court also held that a jury could find that Panuwat breached a fiduciary duty when trading (a necessary component of a misappropriation theory of insider trading) on three potential grounds: (i) Medivation’s insider trading policy, which broadly prohibited trading *in any company* on the basis of confidential information; (ii) Medivation’s confidentiality policy; and (iii) Panuwat’s general duties as an employee of Medivation. As we described in our [alert](#), although the SEC described its theory as standard insider trading, there is no doubt that *Panuwat* expanded potential insider trading liability, with broad implications for future civil and criminal enforcement.

Recordkeeping

To date, in 2024, the SEC has brought three additional rounds of settlements with broker-dealers and investment advisers as part of its ongoing sweep relating to recordkeeping and off-channel communications. Firms have paid a combined total of over \$480 million in penalties in 2024, and over \$3 billion in fines as part of the overall sweep. Each of the firms have also agreed to retain independent compliance consultants to conduct comprehensive reviews of their implementation and enforcement of policies and procedures related to the retention of electronic communications on personal devices. Notably, the firms admitted the facts in the SEC’s orders.

- In February, the SEC announced settled charges against five broker-dealers, seven dually registered broker-dealers and investment advisers, and four affiliated investment advisers for failing to maintain and preserve electronic communications.[\[1\]](#)
- In April, the SEC announced settled enforcement charges against a registered investment adviser for alleged recordkeeping and ethics code violations.[\[2\]](#)
- In August, the SEC announced settled charges against 26 broker-dealers, investment advisers, and dually-registered broker-dealers and investment advisers.[\[3\]](#)

The SEC has used its recordkeeping sweep enforcement efforts as an example of the benefits of cooperation. In his remarks at SEC Speaks in April, Deputy Director of Enforcement Sanjay Wadhwa noted that self-reporting is “the most significant factor in moving the needle on penalties” in the recordkeeping matters.[\[4\]](#) In its August announcement, the SEC noted that three of the firms paid significantly lower civil penalties, ranging from \$400,000 to \$1.6 million, as a result of self-reporting, which Director of Enforcement Gurbir Grewal described as “demonstrating once again the real benefits of proactive cooperation.”[\[5\]](#)

Whistleblower Protection

In 2024, the SEC has also continued to expand the scope of what it interprets as a violation of whistleblower protection rules under Exchange Act Rule 21F. In January, the SEC announced settled charges against a broker-dealer for allegedly violating Rule 21F not with respect to its employees, but to its *clients*.[\[6\]](#) Moreover, the information that the broker-dealer allegedly forbade individuals from disclosing did not relate broadly to the broker-dealer’s operations or financial undertakings, but instead related narrowly to the contents of specific release agreements between the clients and the broker-dealer. The SEC order alleged that, from March 2020 to July 2023, the broker-dealer asked retail clients to sign release agreements through which clients promised “not to sue or solicit others to institute any action or proceeding against

[the broker-dealer] arising out of events concerning the Account.” With respect to the alleged Rule 21F violations, the release agreements included a clause requiring clients to “keep t[he] Agreement confidential and not use or disclose the allegations, facts, contentions, liability, damages, or other information relating in any way to the Account, including but not limited to, the existence or terms of t[he] Agreement.” Though the clause also included a carveout that “neither prohibited nor restricted [clients] from responding to any inquiry about t[he] settlement or its underlying facts by FINRA, the SEC, or any other government entity,” the SEC alleged that the carveout was not expansive enough, and that the release agreements nonetheless prohibited clients from “affirmatively reporting” information to the Commission staff. Without admitting or denying the SEC’s findings, the broker-dealer agreed to pay an \$18 million civil penalty.

The above enforcement action marks yet another instance where the SEC expanded the scope of the types of conduct it perceives as violating Rule 21F. For example, even confidentiality agreements between an entity and its external clients (as opposed to internal employees with more intimate knowledge of the entity) are subject to the rule. Moreover, it seems that any confidentiality clause, regardless of how narrow its scope, may fall within the seemingly expanding contours of whistleblower protection. Though it is unclear from publicly available materials whether the confidentiality clause in the above action related narrowly to the information in the release agreement and its underlying facts, or more broadly to any information about the clients’ accounts, the SEC’s discussion throughout the order implied that the Commission may require whistleblower carveout clauses for any confidentiality agreement, no matter how narrow.

B. Litigation Setbacks

In June and July 2024, the SEC suffered a number of notable litigation setbacks, including decisive decisions vacating the SEC’s proposed private funds rule and prohibiting the use of the SEC’s in-house courts when seeking civil penalties for fraud. A recent ruling in the SolarWinds case also casts doubt—echoing the sentiments voiced by Commissioners Peirce and Uyeda—on the SEC’s ability to continue to use the internal accounting controls provision as a wide-ranging hammer in enforcement matters.

Private Funds Rule

In June, a unanimous panel of the Fifth Circuit vacated the SEC’s proposed private funds rule. As described in our [alert](#) on the ruling, the Court held that the rule exceeded the SEC’s statutory authority. The SEC’s proposed rule would have required a host of restrictions on private funds. Gibson Dunn represented the petitioners in the Fifth Circuit case.

In-House Courts

Also in June, the Supreme Court held 7-3 in *SEC v. Jarkesy* that the Seventh Amendment requires the SEC to sue in federal court when seeking civil penalties for fraud. As described in our [2023 Mid-Year alert](#), the Court held that the SEC’s prior use of its in-house adjudication process was unconstitutional. Although the decision may have little impact on pending enforcement actions (given that the SEC has not recently pursued actions in its in-house

tribunals), there is no doubt that the decision alters the calculus going forward of whether to settle with the SEC by putting defendants on equal footing with the government before a federal court.

Internal Accounting Controls

In June 2024, the SEC announced settled charges against a public company that was the subject of a ransomware attack for alleged violations of the internal accounting controls and disclosure controls provisions of the federal securities laws.^[7] As we described in our [alert](#) regarding the action, the SEC's order, which alleged that the company failed to develop and maintain a system of cybersecurity-related internal accounting controls sufficient to prevent unauthorized access to the company's information technology systems and networks, is notable for extending the internal controls provisions of Section 13(b)(2)(B) of the Exchange Act to a company's IT systems. The SEC had previously brought actions in 2020 and 2023 using the same provision to bring cases relating to stock buybacks and Rule 10b5-1 plans. As with those cases, the action brought a strongly-worded dissent from Commissioners Hester Peirce and Mark Uyeda criticizing "the Commission's decision to stretch the law to punish a company that was the victim of a cyberattack."^[8]

One month later, in a separate ongoing litigation, the United States District Court for the Southern District of New York largely granted SolarWinds' motion to dismiss the SEC's claims in a litigation against the company and its former Chief Information Security Officer (CISO) propounding a similar theory of liability. Specifically, as described in our [alert](#) concerning the case, the Court dismissed the SEC's claim that cybersecurity-related deficiencies are actionable under rules relating to internal accounting and disclosure controls. The Court echoed the prior views of Commissioners Peirce and Uyeda, noting that "[a]s a matter of statutory construction, [the SEC's] reading is not tenable." The Court's decision calls into question the SEC's attempts to adopt an expansive reading of its rules relating to internal accounting controls and disclosure controls.

C. Senior Staffing Update

The Commission has already announced notable staff updates in Fiscal Year 2024 and has also publicized plans to shut down one of its regional offices.

Just before the turn of the year, Mark T. Uyeda was sworn in as a Commissioner for a second term, which expires in 2028.^[9] Commissioner Uyeda first joined the SEC in 2006 as a staff member, and subsequently served in various roles—including as Senior Advisor to Chairman Jay Clayton, Senior Advisor to Acting Chairman Michael S. Piwowar, and Counsel to Commissioner Paul S. Atkins—before becoming a Commissioner in 2022. Prior to his service with the SEC, Commissioner Uyeda served as Chief Advisor to the California Corporations Commissioner and worked as an attorney for several law firms.

In June, the SEC announced the appointment of Erica Y. Williams to a second term as Chair of the Public Company Accounting Oversight Board (PCAOB), which will run from October 25, 2024, and through October 24, 2029.^[10] Prior to joining the PCAOB in January 2022, Chair Williams was a litigation partner at a law firm, and had previously served in various roles at the SEC, including as Deputy Chief of Staff to three former SEC Chairs and Assistant Chief Litigation

Counsel in the SEC's Division of Enforcement trial unit. Chair Williams also served as Special Assistant and Associate Counsel to President Barack Obama.

There were also several changes at the senior staff level and in regional leadership, including within the Division of Investment Management, Office of the Advocate for Small Business Capital Formation, Office of Minority and Women Inclusion, and other policy and office directors:

- In January, Stacey Bowers was named director of the SEC's Office of the Advocate for Small Business Capital Formation (OASB), which was formed in January 2019 as an independent office aimed to promote the interests of small businesses and their investors during the capital formation process.^[11] This is not Ms. Bowers' first time serving with the Commission; she began her legal career at the SEC as a staff attorney in the Division of Corporation Finance before leaving for private practice. From 2007 until becoming the Director of OASB, Ms. Bowers was a law professor at the University of Denver's Sturm College of Law and served as the Director of the Corporate and Commercial Law Program since 2018.
- In March, Natasha Vij Greiner, the former Deputy Director of the Division of Examinations, became Director of the Division of Investment Management, which regulates investment advisers and investment companies.^[12] Greiner has served in various roles in the SEC for over 22 years including Acting Chief Counsel and Assistant Chief Counsel in the Division of Trading and Markets. As Director of the Division of Investment Management, Ms. Greiner replaced William Birdthistle, who joined the SEC in December 2021 and oversaw the adoption of major rulemakings related to public and private funds. Mr. Birdthistle left the SEC to teach law at the University of Chicago.
- In May, the SEC announced the appointment of Nathaniel H. Benjamin to be the Director of the Office of Minority and Women Inclusion (OMWI) and replace Allison Wise, who is OMWI's Deputy Director and had been serving as Acting Director since October 2023.^[13] Benjamin previously served as Chief Diversity and Inclusion Officer of AmeriCorps and Deputy Chief Human Capital Officer at the Department of Education, and also served in similar roles at the Office of Management and Budget and the U.S. Department of State.
- In May, the SEC named Tina Diamantopoulos as Director of the Chicago Regional Office.^[14] Diamantopoulos joined the Enforcement Division in the Chicago Regional Office in 1994, and has since served in various roles, including Branch Chief, Senior Special Counsel in the Examinations Division, Counsel to the Regional Director, and Associate Director for the regional broker-dealer examination program.
- In May, the SEC announced the departure of Policy Director Heather Slavkin Corzo, who joined the SEC in April 2021 to lead the policy team, and who oversaw the proposal and adoption of almost 40 rulemakings.^[15] Corey Klemmer, who joined the SEC in 2021 and served as the former Corporation Finance Counsel to Chairman Gary Gensler, was appointed to fill Ms. Corzo's role.

Separately, the SEC announced the pending closure of its Salt Lake Regional Office (SLRO), which is expected to occur later this year due to budget and organizational efficiency concerns.^[16] Current SLRO staff will be aligned to existing SEC organizational components upon the office's closure, and the enforcement jurisdiction over the state of Utah will be shifted to

the SEC's Denver Regional Office. The Commission said it has no plans to close any additional regional offices.

II. PUBLIC COMPANY ACCOUNTING, FINANCIAL REPORTING, AND DISCLOSURE

A. Financial Reporting

In February, the SEC announced settled accounting fraud charges against a China-based technology company, whose American depository shares formerly traded on the New York Stock Exchange, for allegedly violating antifraud, reporting, recordkeeping, and internal controls provisions of the federal securities laws.^[17] According to the SEC's order, from May 2021 through February 2022, two senior managers of the company allegedly orchestrated a fraudulent scheme to prematurely recognize revenue on service contracts, and to improperly recognize revenue on contracts for which the company had not completed work. The SEC alleged that as a result of the managers' alleged misconduct, the company overstated its unaudited financial results for the second and third quarters of 2021 and its announced revenue guidance for the fourth quarter of 2021. Without admitting or denying the allegations, the company agreed to cease and desist from further violations of the charged securities laws. The SEC did not impose civil penalties because the company self-reported the accounting issues, provided extensive cooperation, and took remedial measures, including firing or disciplining those involved in the alleged scheme, reorganizing departments engaged in the misconduct, strengthening accounting controls, and recruiting new finance and accounting staff.

In March, the SEC announced settled charges against a California-based footwear company for violations of related person transaction disclosure requirements, as well as reporting and proxy solicitation provisions, of the federal securities laws.^[18] The SEC's order alleged that, from 2019 through 2022, the company allegedly failed to disclose payments for the benefit of its executives and their immediate family members, the company's employment of two relatives of its executives, and a consulting relationship involving an individual sharing a household with a company executive. The company allegedly further failed to disclose that two of its four executives owed more than \$120,000 to the company for multiple years in relation to personal expenses paid for by the company, but subject to reimbursement by the executives. Without admitting or denying the SEC's allegations, the company agreed to pay a \$1.25 million civil penalty.

B. Public Statements and Disclosures

In January, the SEC announced settled charges against a U.S.-based special purpose acquisition company (SPAC) for allegedly making misleading statements in forms filed with the SEC as part of its January 2021 initial public offering (IPO).^[19] The SEC's order alleged that, despite a statement in the SPAC's SEC filings that the company had not initiated any substantive discussions with potential target companies prior to the IPO, the SPAC discussed a potential business combination with a target company starting in December 2020. The SEC's order further alleged that, after announcing a merger agreement with the target company, the SPAC did not adequately disclose its interactions with the target company in its Form S-4 filings. Without

admitting or denying the allegations, the SPAC agreed to pay a \$1.5 million penalty in the event it closes a merger transaction.

In February, the SEC filed fraud charges against the former CEO and co-founder of a Florida-based advertising technology company for allegedly making materially misleading false statements on social media regarding the company's financial and performance metrics to elevate the company's stock price.^[20] The SEC's complaint alleges that, shortly after the company's May 2021 initial public offering, the former CEO submitted a post on social media that misrepresented company revenues to be between \$10 million and \$20 million, even though the company was set to report \$17,450 in revenue for 2021. Soon thereafter, the former CEO allegedly falsely misrepresented in a YouTube interview that the company was entering into a new contract with the founder of a restaurant chain, though no contract existed and no related discussions had taken place. The SEC's complaint further alleges that, in August 2021 when the company's stock price opened at its lowest level in almost two months, the former CEO made misleading false statements on social media and in a company-issued press release that the company's projected available advertising inventory for 2021 as more than \$100 million, when at the time the company had less than \$5 million in advertising inventory. The SEC's complaint, which is continuing to litigations, seeks a permanent injunction, an officer-and-director bar, and a civil penalty against the former CEO.

In late February, the SEC announced settled charges against an American electric vehicle automaker for violations of antifraud, proxy, and reporting provisions of the federal securities laws by allegedly misleading investors about the company's flagship electric vehicle.^[21] The SEC's order alleged that the company exaggerated demand for the vehicle by obtaining over 100,000 "pre-orders" from non-serious customers that never intended to purchase the vehicles. The SEC's order also alleged that the company misrepresented the delivery timeline for the vehicle by failing to account for production delays, partially due to the company's inability to access critical parts. Though the SEC's investigation remains ongoing, the company agreed—without admitting or denying the SEC's findings—to pay disgorgement of \$25.5 million, subject to bankruptcy court approval.

The SEC also announced settled charges in a related administrative proceeding against the company's former auditor for violating auditor independence standards.^[22] The SEC's order alleged that, prior to the company becoming public in 2020 through merging with a SPAC, the auditor provided certain non-audit services, including financial statement services and bookkeeping, during the company's audit. The auditor then audited the same financial statements related to the company's merger with the SPAC, thus allegedly violating auditor independence standards of the SEC and the PCAOB. Without admitting or denying the allegations, the auditor agreed to a censure, a cease-and-desist order, payment of over \$80,000 in civil penalties, disgorgement, and certain undertakings to improve policies and procedures.

C. Auditors and Accountants

In May, the SEC announced settled charges against a Colorado-based audit firm and its owner for violations of antifraud, recordkeeping, and other provisions of the federal securities laws, by allegedly failing to comply with PCAOB standards in hundreds of audits and reviews, and in thousands of SEC filings, on behalf of hundreds of clients from January 2021 through June

2023.^[23] The SEC's order alleged that the audit firm and owner misrepresented to clients their compliance with PCAOB standards, fabricated documents to appear compliant, and falsely claimed adequate compliance in over 500 public company SEC filings. With respect to the owner, the SEC's order alleged that he failed to adequately prepare and maintain audit documentation, resulting in the firm's lack of quality reviews of audits, and the false documentation of uncompleted work. Without admitting or denying the SEC's findings, the audit firm and owner settled the charges—agreeing to pay civil penalties of \$12 million and \$2 million, respectively, and to a permanent accounting bar.

III. INVESTMENT ADVISERS

A. Misleading Statements and Disclosures

In January, the SEC announced settled charges against a Chicago-based registered investment adviser and one of its former partners for allegedly misleading a client regarding investment returns.^[24] The SEC order alleged that, in June 2020, the company and the partner misled a public-school pension fund as to the reason for a discrepancy between investment returns. Without admitting or denying the SEC's findings, the company agreed to settle the charges and pay over \$1.5 million in penalties and disgorgement, and the former partner agreed to settle the charges and pay a civil penalty of \$30,000.

In February, the SEC announced settled charges against a registered investment adviser for failing to disclose certain details to a client about how it planned to launch the client's product.^[25] The SEC order alleged that, in March 2021, the adviser failed to inform the Board of an exchange-traded fund (ETF) about a social media influencer's role in the launch of the ETF. The investment adviser also allegedly did not inform the ETF Board about the sliding-scale fee structure under which the provider of the ETF-tracked index would receive a greater proportion of the ETF-paid management fees based on how much the fund grew. Without admitting or denying the SEC's findings, the investment adviser agreed to settle the charges and pay a \$1.75 million civil penalty.

In June, the SEC filed charges against an investment management firm and its founder for allegedly defrauding investors of at least \$3 million.^[26] The SEC's complaint alleged that, from 2020 to 2023, the firm and its founder raised at least \$3 million from investors by lying about nearly every aspect of the fund, and then used over \$1 million on personal expenses, lost more than \$1.7 million on high-risk trading and speculative investments, and falsified documents to conceal the trading losses from investors. The firm and its founder settled the civil charges, agreeing to permanent injunctions and to pay disgorgement and civil penalties determined by the court. The company's founder has also pleaded guilty to related criminal charges brought against him by the U.S. Attorney's Office for the District of New Jersey.

B. Marketing Rule

In April, the SEC announced settled charges against five registered investment advisers for Marketing Rule violations.^[27] The SEC's orders alleged that the five firms advertised hypothetical performance to the general public on their websites without adopting and implementing policies and procedures reasonably designed to ensure that the hypothetical

performance was relevant to the likely financial situation and investment objectives of each advertisement's intended audience, as required by the Marketing Rule. One of the firms allegedly committed additional securities laws violations by making false and misleading statements in advertisements, failing to enter into written agreements with people it compensated for endorsements, and committing recordkeeping and compliance violations. Without admitting or denying the SEC's findings, all five firms agreed to settle the charges regarding alleged violations of the Investment Advisers Act of 1940, to pay civil penalties totaling \$200,000, and to comply with certain undertakings. Four of the firms received reduced penalties for taking corrective steps in advance of being contacted by the SEC, and they resultingly paid civil penalties ranging from \$20,000 to \$30,000. The other firm, which was the firm alleged to have committed additional regulatory violations beyond the Marketing Rule violations, agreed to pay a civil penalty of \$100,000.

C. Conflicts of Interest

In May, the SEC announced settled charges against a New York-based registered investment adviser and its owner for breaching fiduciary duties by allegedly failing to disclose conflicts of interest and making misleading statements to clients.^[28] The SEC's order alleged that, between September 2017 and October 2021, the company and the owner advised certain clients to invest in films produced by a particular film production company without disclosing that the adviser would receive payments from the production company in exchange for the money the clients invested in the films. The adviser and owner then later allegedly misrepresented to clients that such payments to the owner were for work as an executive producer on the films. The SEC's order also alleged that the firm and its owner satisfied a redemption request from one client but not from several others submitted at the same time, and that by preferencing one client over the others they violated their fiduciary duties to the other clients. The adviser and owner agreed to settle the charges, which involved alleged violations of the antifraud provisions of the Investment Advisers Act—with the firm agreeing to pay a civil penalty of \$200,000, and the owner agreeing to pay disgorgement and penalties totaling more than \$750,000.

Also in May, the SEC announced settled charges against a New York-based, formerly registered investment adviser and its co-founder and CEO for making false and misleading statements to investors.^[29] The SEC's orders alleged that, from 2020 to 2022, the firm made a series of materially false and misleading statements about its flagship opportunity fund's holdings and exposures. The SEC's orders alleged that these statements were the result of modifications the co-founder and CEO made to underlying portfolio data which was then included in various investor communications. The firm allegedly also did not report to investors a conflict of interest arising from its other co-founder's operation of a separate hedge fund in China. Without admitting or denying the SEC's findings, the firm and the co-founder and CEO agreed to settle the charges, which involved alleged violations of the antifraud and compliance provisions of the Investment Advisers Act—with the firm agreeing to pay a civil penalty of \$350,000, and the co-founder and CEO agreeing to pay a civil penalty of \$250,000 and undergo a 12-month suspension from industry-related work.

D. Beneficial Ownership Rules

In March, the SEC announced settled charges against a New York-based investment adviser for its alleged failure to make timely ownership disclosures in the lead-up to its May 2022 acquisition bid for a publicly traded trucking fleet company.^[30] The SEC's order alleged that the investment adviser increased its position in the trucking company and formed a control purpose no later than April 26, 2022, requiring it to report that information by May 6, 2022, but that it did not do so until May 13, 2022. Additionally, before the time it reported its control purpose, the investment adviser allegedly purchased swap agreements giving it economic exposure to the equivalent of 450,000 more shares of the trucking fleet company's stock. Further, according to the order, when the investment adviser eventually reported the information, it allegedly proposed to buy all the trucking fleet company's shares for a sizable premium over the trading price, and the trucking company's stock price increased significantly. Without admitting or denying the SEC's findings, the investment adviser settled the charges alleging violations of the beneficial ownership provisions of the Securities Exchange Act of 1934, and agreed to pay a \$950,000 civil penalty.

IV. BROKER-DEALERS

A. Regulation Best Interest and Pricing

In February, the SEC announced settled charges against a broker-dealer for failing to comply with Regulation Best Interest (Reg BI), allegedly causing investors to collectively incur hundreds of thousands of dollars in combined expenses.^[31] According to the SEC order, the broker-dealer allegedly disclosed to investors that for certain funds it only offered certain share classes, and failed to inform investors that equivalent, lower-cost share classes for affiliated funds were also available. As a result, a portion of investors paid higher expenses for certain funds that they could have avoided by purchasing substantially similar funds. Without admitting or denying the findings, the broker-dealer agreed to pay a combined total of \$2.2 million in disgorgement and civil penalties.

We predicted in an [alert](#) in June that the SEC would pursue more Reg BI cases, particularly on the conflicts and duty of care elements of the Rule. In late July, the SEC charged a dual registrant for "a risky day trading strategy" one of its registered representatives employed for several of his customers.^[32] The trading strategy involved the purchase and sale of options contracts for customers, some of whom had "moderate to conservative risk profiles." The SEC imposed a relatively small penalty of \$140,000, but specifically noted (1) the firm's cooperation (e.g., disclosing information about conduct the Staff had not yet uncovered, conducting an internal investigation, regularly briefing the Staff regarding its investigation, identifying key documents found in its investigation, and voluntarily providing tables summarizing information from these documents), and (2) the firm's remediation, including "changes to senior management, the \$9 million in financial remediation paid to affected customers, and substantive improvements in [the firm's] policies and procedures," as mitigating factors.

B. Disclosure Obligations

In May, the SEC announced settled charges against an American multinational financial services company and nine of its affiliates.^[33] According to the SEC order, following a cyber intrusion, the company allegedly failed to alert the appropriate legal and compliance officials promptly. As a result, the company and its affiliates allegedly did not inform the Commission within the

required period, violating regulatory disclosure obligations. Without admitting or denying the Commission's findings, the company and its affiliates consented to the SEC's order and agreed to pay a \$10 million penalty.

In June, the SEC charged three individuals who allegedly engaged in a multi-year scheme defrauding investors by selling unregistered membership interests in LLCs investing in shares of two pre-IPO companies.^[34] The complaint alleged that from mid-2019 to early 2022, the individuals directed an unregistered sales force to pressure investors into making investments without disclosing substantial markups on the shares. The individuals further allegedly misled investors by overstating their research capabilities and market projections, violating antifraud and other provisions of the federal securities laws. The complaint seeks permanent injunctive relief, disgorgement, and civil penalties, and litigation is ongoing.

V. CRYPTOCURRENCY AND ARTIFICIAL INTELLIGENCE

The SEC's enforcement activity in the crypto space has remained active but has slowed compared to past periods and has changed form. In the past, the Commission focused its efforts on enforcing what it does, and does not, believe qualifies as a security under the securities laws. Such enforcement efforts have remained in place, but the SEC now has seemingly begun to shift its enforcement efforts toward entities and individuals it believes are taking advantage of the novelty of the crypto space, and other emerging informational and technological advances, such as artificial intelligence, to secure improper investments and investor proceeds.

A. Cryptocurrency

In January, the SEC charged two individuals with violating the antifraud and registration provisions of the federal securities laws for allegedly operating a crypto asset pyramid scheme.^[35] According to the SEC's complaint, from mid-2020 to early 2022, both individuals allegedly lured investors with promises of high profits despite lacking any genuine revenue source other than the funds received from investors. The complaint seeks permanent injunctive relief, conduct-based injunctions prohibiting the defendants from engaging in multi-level marketing or offering crypto assets, disgorgement, and civil penalties. One of the individuals settled the charges and agreed to pay disgorgement and civil penalties to be announced at a later court date.

In February, the SEC charged a company and its founder with violating the antifraud provisions under the federal securities laws through an alleged scheme targeting students of the founder's online crypto trading course.^[36] From early 2018 to mid-2019, the founder allegedly encouraged hundreds of students to invest in the founder's hedge fund he claimed would utilize advanced strategies to secure profits. The SEC alleged that the founder never launched the fund or executed the advertised strategies, instead holding the invested money in bitcoin. Without admitting or denying the allegations, the defendants consented to injunctive relief and agreed to pay \$1.2 million in disgorgement and civil penalties.

Also in February, the SEC announced settled charges against a broker-dealer for allegedly failing to register the offer and sale of a crypto lending product that allowed investors to deposit or purchase crypto assets in their account in exchange for the company's promise to pay

interest.^[37] According to the SEC order, from late 2020 to early 2022, the broker-dealer allegedly offered a crypto lending product intended to generate revenue to pay interest to investors. However, the broker-dealer allegedly sold this product as a security without registering it, violating registration provisions of the federal security laws. Without admitting or denying the SEC's findings, the broker-dealer agreed to pay \$1.5 million in civil penalties.

In March, the SEC announced final judgment against a financial services company for violating disclosure requirements by allegedly failing to register its retail crypto lending product before offering it to the public.^[38] The SEC further alleged that the company was unable to liquidate its assets when investors sought to withdraw their funds due to the volatility of the crypto market. Without admitting or denying the allegations, the company settled charges and agreed to pay \$21 million in civil penalties.

In June, the SEC announced settled fraud charges against a publicly traded South Korean crypto asset company and its co-founder.^[39] According to the SEC's order, the company allegedly misrepresented the use of its blockchain for transaction settlements and the stability of its crypto asset security, violating antifraud provisions of the federal securities laws. The SEC further alleged that in May 2022, after the company's token asset de-pegged from the U.S. dollar, the value of the token and the company's other tokens plummeted to near zero, allegedly wiping out \$40 billion in market value overnight and causing significant losses to investors. The company settled the charges, which included allegations of securities fraud and the offering and selling of securities in unregistered transactions, agreeing to pay a combined total of \$4.5 billion in disgorgement and civil penalties. The company also agreed to cease the sale of its crypto asset securities, wind down its operations, replace two of its directors, and distribute its remaining assets to investor victims and creditors. The company's co-founder also settled charges and agreed to pay a combined total of \$204 million in disgorgement and civil penalties.

B. Artificial Intelligence

In March, the SEC announced settled charges against two investment advisers, one Toronto-based and the other San Francisco-based, for allegedly making false and misleading statements about their purported use of artificial intelligence (AI).^[40] The SEC's order against the Toronto-based firm alleged that, from 2019 to 2023, it violated the marketing rule and made false and misleading statements in its SEC filings, in a press release, and on its website regarding its purported use of AI and machine learning capabilities that it did not in fact have. The SEC's order against the San Francisco-based firm similarly alleged that the firm made false and misleading claims in 2023 on its website and on social media about its purported use of AI, and that it violated the Marketing Rule by, among other things, falsely claiming it offered tax-loss harvesting services. Without admitting or denying the SEC's findings, both firms agreed to settle the charges against them, which involved violations of the Advisers Act—with the Toronto-based firm agreeing to pay a civil penalty of \$225,000, and the San Francisco-based firm agreeing to pay a civil penalty of \$175,000.

In June, the SEC charged the CEO of an artificial intelligence recruitment startup who allegedly made false and misleading statements in a multi-year scheme that defrauded investors.^[41] According to the complaint, from 2018 to mid-2023, the CEO allegedly lied to investors about the quantity and quality of customers, the number of candidates on the platform,

and the company's revenue, violating the antifraud provisions of the federal securities laws. The complaint seeks a permanent injunction, civil monetary penalties, disgorgement, and an officer-and-director bar against the company's CEO. Additionally, the U.S. Attorney's Office for the Southern District of New York brought criminal charges against the CEO in a parallel action.

VI. INSIDER TRADING AND MARKET MANIPULATION

The SEC has continued to aggressively investigate potential insider trading. The Commission's enforcement in this area will likely maintain its pace, given not only the trends that are prevalent, but also the SEC's victory at trial in April 2024 in the *Panuwat* case discussed *supra*.

In January, the SEC announced settled charges against an investment bank and its former head of equity syndicate chair for their alleged involvement in an alleged multi-year fraud related to the disclosure of purportedly confidential information about block trades and alleged failure to enforce policies regarding the misuse of material non-public information related to the block-trades.^[42] According to the SEC's order, from mid-2018 to mid-2021, the investment bank and former head allegedly disseminated non-public information concerning upcoming block trades, violating federal securities laws. The SEC further alleged that the investment bank failed to enforce information barriers that would have prevented the former head from disseminating the information. Both the investment bank and the former equity syndicate chair settled the charges; the bank agreed to pay a combined total of \$249 million in disgorgement and civil penalties (which were partially satisfied by payments in a parallel action brought by the U.S. Attorney's Office for the Southern District of New York). The Southern District of New York resolved its criminal investigation pursuant to a Non-Prosecution Agreement with the bank, and Deferred Prosecution Agreement with the former equity syndicate chair.

Also in January, the SEC charged the CEO of a China-based FinTech company with violating the antifraud and beneficial ownership provisions of the Securities Exchange Act of 1934.^[43] The SEC's complaint alleged that the CEO manipulatively traded company stock through an offshore account prior to becoming CEO in 2020 to raise the company stock price, and that the CEO failed to disclose his beneficial ownership of, and transactions in, company stock. According to the complaint, in late 2019 or early 2020, the founder and former CEO of the company approached the current CEO with the prospect of taking over the CEO position. At that time, the company risked delisting from NASDAQ due to its stock price falling below the minimum \$1.00 per share bid price requirement. Beginning in January 2020 and prior to becoming CEO, the current CEO allegedly traded company stock through a Hong Kong account, purchasing more than 530,000 shares of company stock over the next two-month period—allegedly making nonsensical trades at such a high volume that they comprised a high percentage of daily volume of company stock transactions—with the intent and eventual effect of driving the stock price up. Then, upon becoming CEO in March 2020, the CEO allegedly failed to file change of ownership forms regarding his holdings of company stock. Similarly, the following year after he allegedly no longer owned any company stock, the CEO belatedly filed a misleading initial form representing that he owned no company stock. The SEC is seeking permanent injunctive relief, a civil penalty, and an officer-and-director bar, in the ongoing litigation.

In February, the SEC filed charges against the husband of an energy company manager for allegedly trading on material, nonpublic information about a proposed acquisition the energy

company planned to execute.^[44] The individual allegedly overheard his wife's work-related conversations about the proposed acquisition and executed trades based on that information in February 2023 without his wife's knowledge, for a profit of \$1.76 million. The individual agreed to the entry of a partial judgment permanently enjoining him from violating the antifraud provisions of the federal securities laws, barring him from acting as an officer or director of a public company, and requiring him to pay disgorgement and an undetermined civil penalty. The SEC's investigation is still ongoing, and the U.S. Attorney's Office for the Southern District of Texas has brought charges against the individual in a parallel action.

In March, the SEC announced charges against a former board member of an energy company, along with four of his associates, for allegedly trading on material nonpublic information.^[45] According to the complaint, in July 2019, the former board member learned of a pending investment offered to privatize the energy company. The former board member and four of his associates then allegedly purchased company securities prior to the public announcement of the offer, and then traded the shares to earn gains totaling tens of thousands of dollars. The former board member settled with the SEC, agreeing to a \$801,742 civil penalty plus disgorgement, along with an officer and director bar. The four other defendants each agreed to pay civil penalties plus disgorgement.

In March, the SEC filed insider trading charges against the founder of a technology company regarding trades he made in July 2019 that earned profits of \$415,726.^[46] The individual allegedly learned from a friend about a multinational technology company's pending acquisition of a communications equipment company, and then he allegedly traded options for the target company through a close relative and an associate. The individual settled with the SEC and agreed to a civil penalty of \$923,740 and a five-year officer and director bar.

In May, the SEC charged an individual with violations of the securities laws for allegedly trading on inside information about a publicly traded company that resulted in profits of more than \$800,000.^[47] According to the complaint, between November 2019 and May 2021, the individual solicited updates from a company employee on the company's performance. Then, despite requests from the employee not to trade company securities, the individual allegedly used the information to trade in the company's securities. The individual settled with the SEC and agreed to pay disgorgement, prejudgment interest, and a civil penalty to be determined by the U.S. District Court for the Western District of Pennsylvania. The U.S. Attorney's Office for the Western District of Pennsylvania also brought criminal charges against the individual in a parallel action.

In May, the SEC charged a Massachusetts-based venture investment company and its founder with violations of antifraud provisions under the federal securities laws arising from an alleged scheme to artificially inflate the stock price of a Seattle-based visual media company.^[48] The SEC's complaint alleged that in April 2023, the founder and venture investment company issued a press release offering to purchase all outstanding stock of the media company for \$10 a share, almost double the closing price of the previous trading day, which allegedly caused the company's stock price to spike. Though the founder and his company allegedly pledged in the press release to hold their shares, they allegedly began liquidating stock in the visual media company shortly after the market opened on April 24, 2023, before the media company responded to the offer. The founder and venture investment company settled the charges—

agreeing to pay civil penalties and disgorgement to be determined by the court, along with an officer and director bar. In a parallel action, the U.S. Attorney's Office for the District of Massachusetts announced criminal charges against the founder of the venture investment company.

[1] SEC Press Release, Sixteen Firms to Pay More Than \$81 Million Combined to Settle Charges for Widespread Recordkeeping Failures (February. 9, 2024), *available at* <https://www.sec.gov/news/press-release/2024-18>.

[2] SEC Press Release, SEC Charges Advisory Firm Senvest Management with Recordkeeping and Other Failures (Apr. 3, 2024), *available at* <https://www.sec.gov/news/press-release/2024-44>.

[3] SEC Press Release, Twenty-Six Firms to Pay More Than \$390 Million Combined to Settle SEC's Charges for Widespread Recordkeeping Failures (Aug. 14, 2024), *available at* <https://www.sec.gov/newsroom/press-releases/2024-98>.

[4] SEC Speech, Remarks at SEC Speaks 2024, Sanjay Wadhwa, Deputy Director, Division of Enforcement (Apr. 3, 2024), *available at* <https://www.sec.gov/newsroom/speeches-statements/sanjay-wadhwa-sec-speaks-2024-04032024>.

[5] SEC Press Release, Twenty-Six Firms to Pay More Than \$390 Million Combined to Settle SEC's Charges for Widespread Recordkeeping Failures (Aug. 14, 2024), *available at* <https://www.sec.gov/newsroom/press-releases/2024-98>.

[6] SEC Press Release, J.P. Morgan to Pay \$18 Million for Violating Whistleblower Protection Rule (Jan. 16, 2024), *available at* <https://www.sec.gov/news/press-release/2024-7>.

[7] SEC Press Release, SEC Charges R.R. Donnelley & Sons Co. with Cybersecurity-Related Controls Violations (June 18, 2024), *available at* <https://www.sec.gov/news/press-release/2024-75>.

[8] SEC Statement, Hey, look, there's a hoof cleaner! Statement on R.R. Donnelley & Sons, Co., Commissioners Hester M. Peirce and Mark T. Uyeda (June 18, 2024), *available at* <https://www.sec.gov/newsroom/speeches-statements/peirce-uyeda-statement-rr-donnelley-061824>.

[9] SEC Press Release, Mark Uyeda Sworn in for Second Term as SEC Commissioner (Jan. 3, 2024), *available at* <https://www.sec.gov/news/press-release/2024-1>.

[10] SEC Press Release, SEC Appoints Erica Y. Williams to a Second Term as PCAOB Chairperson (Jun. 11, 2024), *available at* <https://www.sec.gov/news/press-release/2024-71>.

[11] SEC Press Release, SEC Appoints Stacey Bowers as Small Business Advocate (Jan. 5, 2024), *available at* <https://www.sec.gov/news/press-release/2024-3>.

[12] SEC Press Release, SEC Announces Departure of William Birdthistle; Natasha Vij Greiner Named Director of the Division of Investment Management (Feb. 28, 2024), *available at* <https://www.sec.gov/news/press-release/2024-27>.

[13] SEC Press Release, SEC Names Nathaniel H. Benjamin as Director of the Office of Minority and Women Inclusion (May 3, 2024), *available at* <https://www.sec.gov/news/press-release/2024-52>.

[14] SEC Press Release, Tina Diamantopoulos Named Regional Director of Chicago Office (May 16, 2024), *available at* <https://www.sec.gov/news/press-release/2024-59>.

[15] SEC Press Release, SEC Announces Departure of Policy Director Heather Slavkin Corzo and Appointment of Corey Klemmer to the Role (May 17, 2024), *available at* <https://www.sec.gov/news/press-release/2024-60>.

[16] SEC Press Release, SEC to Close Salt Lake Regional Office (Jun. 4, 2024), *available at* <https://www.sec.gov/news/press-release/2024-67>.

[17] SEC Press Release, SEC Charges China-Based Tech Company Cloopen Group with Accounting Fraud (Feb. 6, 2024), *available at* <https://www.sec.gov/news/press-release/2024-15>.

[18] SEC Press Release, SEC Charges Skechers with Making Undisclosed Payments to Executives' Family Members (Mar. 7, 2024), *available at* <https://www.sec.gov/news/press-release/2024-33>.

[19] SEC Press Release, SEC Charges Northern Star SPAC for Material Misrepresentations in its IPO-Related Disclosures (Jan. 25, 2024), *available at* <https://www.sec.gov/news/press-release/2024-10>.

[20] SEC Press Release, SEC Charges Former Alfi CEO Paul Pereira with Fraud for Making False Statements on Social Media (Feb. 27, 2024), *available at* <https://www.sec.gov/news/press-release/2024-26>.

[21] SEC Press Release, SEC Charges Lordstown Motors with Misleading Investors about Company's Flagship Electric Vehicle (Feb. 29, 2024), *available at* <https://www.sec.gov/news/press-release/2024-29>.

[22] *Id.*

[23] SEC Press Release, SEC Charges Audit Firm BF Borgers and Its Owner with Massive Fraud Affecting More Than 1,500 SEC Filings (May 3, 2024), *available at* <https://www.sec.gov/news/press-release/2024-51>.

[24] SEC Press Release, SEC Charges Chicago-based Aon Investments and Former Partner with Misleading Pennsylvania Public Employees' Pension Fund (Jan. 25, 2024), *available at* <https://www.sec.gov/news/press-release/2024-9>.

[25] SEC Press Release, SEC Charges Van Eck Associates for Failing to Disclose Influencer's Role in Connection with ETF Launch (Feb. 16, 2024), *available at* <https://www.sec.gov/news/press-release/2024-20>.

[26] SEC Press Release, SEC Charges JAG Capital Advisors and its Founder Joshua Goltry with Defrauding Investors (Jun. 12, 2024), *available at* <https://www.sec.gov/news/press-release/2024-72>; DOJ Press Release, New York Fund Manager Admits Multimillion-Dollar Investment Fraud Scheme (June 12, 2024), *available at* <https://www.justice.gov/usao-nj/pr/new-york-fund-manager-admits-multimillion-dollar-investment-fraud-scheme>.

[27] SEC Press Release, SEC Charges Five Investment Advisers for Marketing Rule Violations (Apr. 12, 2024), *available at* <https://www.sec.gov/news/press-release/2024-46>.

[28] SEC Press Release, SEC Charges Hudson Valley Wealth Management Advisory Firm and Founder for Failing to Disclose Conflicts of Interest (May 14, 2024), *available at* <https://www.sec.gov/news/press-release/2024-55>.

[29] SEC Press Release, SEC Charges Advisory Firm Mass Ave Global and Co-Founder and CEO Winston Feng with False Statements and Undisclosed Conflicts (May 29, 2024), *available at* <https://www.sec.gov/news/press-release/2024-64>.

[30] SEC Press Release, SEC Charges Advisory Firm HG Vora for Disclosure Failures Ahead of Ryder Acquisition Bid (Mar. 1, 2024), *available at* <https://www.sec.gov/news/press-release/2024-30>.

[31] SEC Press Release, SEC Charges TIAA Subsidiary for Failing to Act in the Best Interest of Retail Customers (Feb. 16, 2024), *available at* <https://www.sec.gov/news/press-release/2024-22>.

[32] SEC Order Instituting Administrative and Cease and Desist Proceedings, *In the Matter of Western International Securities, Inc.* (Administrative Proceeding File No. 3-21986) (July 30, 2024), *available at* <https://www.sec.gov/files/litigation/admin/2024/34-100618.pdf>.

[33] SEC Press Release, SEC Charges Intercontinental Exchange and Nine Affiliates Including the New York Stock Exchange with Failing to Inform the Commission of a Cyber Intrusion (May 22, 2024), *available at* <https://www.sec.gov/news/press-release/2024-63>.

[34] SEC Press Release, SEC Charges Three New Yorkers for Raising More Than \$184 Million Through Pre-IPO Fraud Schemes (June 7, 2024), *available at* <https://www.sec.gov/news/press-release/2024-69>.

[35] SEC Press Release, SEC Charges Founder of \$1.7 Billion "HyperFund" Crypto Pyramid Scheme and Top Promoter with Fraud (Jan. 29, 2024), *available at* <https://www.sec.gov/news/press-release/2024-11>.

[36] SEC Press Release, SEC Charges Founder of American Bitcoin Academy Online Crypto Course with Fraud Targeting Students (Feb. 2, 2024), *available at* <https://www.sec.gov/news/press-release/2024-13>.

[37] SEC Press Release, SEC Charges TradeStation Crypto for Unregistered Offer and Sale of Crypto Asset Lending Product (Feb. 7, 2024), *available at* <https://www.sec.gov/news/press-release/2024-16>.

[38] SEC Press Release, Genesis Agrees to Pay \$21 Million Penalty to Settle SEC Charges (Mar. 19, 2024), *available at* <https://www.sec.gov/news/press-release/2024-37>.

[39] SEC Press Release, Terraform and Kwon to Pay \$4.5 Billion Following Fraud Verdict (June 11, 2024), *available at* <https://www.sec.gov/news/press-release/2024-73>.

[40] SEC Press Release, SEC Charges Two Investment Advisers with Making False and Misleading Statements About Their Use of Artificial Intelligence (Mar. 18, 2024), *available at* <https://www.sec.gov/news/press-release/2024-36>.

[41] SEC Press Release, SEC Charges Founder of AI Hiring Startup Joonko with Fraud (June 11, 2024), *available at* <https://www.sec.gov/news/press-release/2024-70>.

[42] SEC Press Release, SEC Charges Morgan Stanley and Former Executive Pawan Passi with Fraud in Block Trading Business (Jan. 12, 2024), *available at* <https://www.sec.gov/news/press-release/2024-6>.

[43] SEC Press Release, SEC Charges Future FinTech CEO Shanchun Huang With Fraud and Disclosure Failures (Jan. 11, 2024), *available at* <https://www.sec.gov/news/press-release/2024-5>.

[44] SEC Press Release, SEC Charges Husband of Energy Company Manager with Insider Trading (Feb. 22, 2024), *available at* <https://www.sec.gov/news/press-release/2024-24>.

[45] SEC Press Release, SEC Charges Tallgrass Energy's Former Board Member Roy Cook and Four Others with Insider Trading in Advance of Blackstone Acquisition (Mar. 12, 2024), *available at* <https://www.sec.gov/news/press-release/2024-34>.

[46] SEC Press Release, SEC Charges Former Arista Networks Chairman Andy Bechtolsheim with Insider Trading (Mar. 26, 2024), *available at* <https://www.sec.gov/news/press-release/2024-40>.

[47] SEC Press Release, SEC Charges Pennsylvania Resident with Insider Trading in Dick's Sporting Goods Securities (May 10, 2024), *available at* <https://www.sec.gov/news/press-release/2024-53>.

[48] SEC Press Release, SEC Charges Robert Scott Murray and Trillium Capital with Fraudulent Scheme to Manipulate Getty Images Stock (May 31, 2024), *available at* <https://www.sec.gov/news/press-release/2024-66>.

The following Gibson Dunn lawyers assisted in preparing this update: Mark Schonfeld, David Woodcock, Tina Samanta, Lauren Jackson, Timothy Zimmerman, and Michael Ulmer.

Gibson Dunn lawyers are available to assist in addressing any questions you may have about these developments. Please contact the Gibson Dunn lawyer with whom you usually work, any leader or member of the firm's Securities Enforcement practice group, or the following authors:

Mark K. Schonfeld – Co-Chair, New York (+1 212.351.2433, mschonfeld@gibsondunn.com)

David Woodcock – Co-Chair, Dallas (+1 214.698.3211, dwoodcock@gibsondunn.com)

Tina Samanta – New York (+1 212.351.2469, tsamanta@gibsondunn.com)

Lauren Cook Jackson – Washington, D.C. (+1 202.955.8293, ljackson@gibsondunn.com)

Timothy M. Zimmerman – Denver (+1 303.298.5721, tzimmerman@gibsondunn.com)

Attorney Advertising: These materials were prepared for general informational purposes only based on information available at the time of publication and are not intended as, do not constitute, and should not be relied upon as, legal advice or a legal opinion on any specific facts or circumstances. Gibson Dunn (and its affiliates, attorneys, and employees) shall not have any liability in connection with any use of these materials. The sharing of these materials does not establish an attorney-client relationship with the recipient and should not be relied upon as an alternative for advice from qualified counsel. Please note that facts and circumstances may vary, and prior results do not guarantee a similar outcome.

If you would prefer NOT to receive future emailings such as this from the firm,
please reply to this email with "Unsubscribe" in the subject line.

If you would prefer to be removed from ALL of our email lists,
please reply to this email with "Unsubscribe All" in the subject line. Thank you.

© 2024 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at gibsondunn.com

GIBSON DUNN

Environmental, Social and Governance Update

November 7, 2024

Gibson Dunn Environmental, Social and Governance (ESG) Update

We are pleased to provide you with Gibson Dunn's ESG update covering the following key developments during October 2024. Please click on the links below for further details.

I. GLOBAL

1. **Taskforce on Nature-related Financial Disclosures (TNFD) publishes guidance on nature transition planning**
2. **International Sustainability Standards Board (ISSB) finalizes updates to the Sustainability Accounting Standards Board (SASB) Standards Taxonomy**

II. UNITED KINGDOM

1. **UK Government issues response on UK Carbon Border Adjustment Mechanism (UK CBAM) consultation**
2. **New duty on UK employers to prevent sexual harassment in the workplace comes into force**
3. **Institute of Directors publishes a voluntary code of conduct for directors**
4. **House of Lords Select Committee publishes its report on The Modern Slavery Act**
5. **UK's cap-and-floor scheme to support energy storage investment**

6. **UK Government publishes its Employment Rights Bill**
7. **UK Government pledges £21.7 billion in funding for carbon capture and storage projects**

III. EUROPE

1. **Sustainability Statements among the European Securities and Markets Authority's (ESMA) Key Three Enforcement Priorities**
2. **EU invests EUR 4.8 billion in Decarbonization Projects Funded by Carbon Pricing**
3. **EU Council agrees to delay the EU Deforestation Regulation (EUDR) Applicability by one year**
4. **Open letter urges EU to establish ambitious investment plan for climate and biodiversity goals**
5. **ESMA published first report on EU Carbon Markets for 2024**
6. **CSRD Transposition is progressing**

IV. NORTH AMERICA

1. **U.S. House bill could alter the reporting of greenhouse gas emissions caused by federal legislation**
2. **The Hershey Company (Hershey) accused of material misrepresentations related to bubble gum product**
3. **New York City Comptroller proposes fossil fuel ban in pension fund investing**
4. **House of Representatives introduces Stop Woke Investing Act**
5. **WisdomTree Asset Management, Inc. (WisdomTree) settles enforcement action related to ESG investment strategy**
6. **SEC seeks comments on Green Impact Exchange, LLC (GIX) registration**
7. **Bill seeks to prevent federal agencies from considering the social cost of carbon and other greenhouse gases in agency action**
8. **Canada to require mandatory climate disclosures for large companies and provide sustainable investment guidelines**
9. **U.S. Commodity Futures Trading Commission (CFTC) files lawsuit alleging carbon credit misrepresentations**

In case you missed it...

The Gibson Dunn [Workplace DEI Task Force](#) has published its updates for October summarizing the latest key developments, media coverage, case updates, and legislation related to diversity, equity, and inclusion.

V. APAC

1. **Asia Investor Group on Climate Change (AIGCC) calls for ambitious energy targets in Japan's 7th Strategic Energy Plan**
2. **Hong Kong unveils Sustainable Finance Action Agenda**
3. **Australia releases Guide on AI for ESG practitioners**
4. **Malaysia's ESG Disclosure Report: Establishing Baseline Standards for Reporting Practices**
5. **Hong Kong Code of Conduct for ESG ratings and data products providers**

[Read More](#)

Warmest regards,

Susy Bullock
Elizabeth Ising
Perlette M. Jura
Ronald Kirk
Michael K. Murphy
Robert Spano

Chairs, [Environmental, Social and Governance Practice Group](#), Gibson Dunn & Crutcher LLP

For further information about any of the topics discussed herein, please contact the ESG Practice Group Chairs or contributors, or the Gibson Dunn attorney with whom you regularly work.

The following Gibson Dunn lawyers prepared this update: Lauren Assaf-Holmes, Carla Baum, Mitasha Chandok, Becky Chung, Georgia Derbyshire, Ferdinand Fromholzer, Muriel Hague, William Hallatt, Beth Ising, Sarah Leiper-Jennings, Vanessa Ludwig, Babette Milz*, Johannes Reul, Annie Saunders, Helena Silewicz*, QX Toh, and Katherine Tomsett.

[ESG Practice Group Leaders and Members](#)



Susy Bullock
London
+44 20 7071 4283
sbullock@gibsondunn.com



Elizabeth A. Ising
Washington, D.C.
+1 202.955.8287
eising@gibsondunn.com



Perlette Michèle Jura
Los Angeles
+1 213.229.7121
pjura@gibsondunn.com



Ronald Kirk
Dallas
+1 214.698.3295
rkirk@gibsondunn.com



Michael K. Murphy
Washington, D.C.
+1 202.955.8238
mmurphy@gibsondunn.com



Robert Spano
London/Paris
+33 1 56 43 13 00
rspano@gibsondunn.com

**Helena Silewicz, a trainee solicitor in London, and Babette Milz, a research assistant in Munich, are not admitted to practice law.*

Attorney Advertising: These materials were prepared for general informational purposes only based on information available at the time of publication and are not intended as, do not constitute, and should not be relied upon as, legal advice or a legal opinion on any specific facts or circumstances. Gibson Dunn (and its affiliates, attorneys, and employees) shall not have any liability in connection with any use of these materials. The sharing of these materials does not establish an attorney-client relationship with the recipient and should not be relied upon as an alternative for advice from qualified counsel. Please note that facts and circumstances may vary, and prior results do not guarantee a similar outcome.

If you would prefer NOT to receive future emailings such as this from the firm, please reply to this email with "Unsubscribe" in the subject line.

If you would prefer to be removed from ALL of our email lists, please reply to this email with "Unsubscribe All" in the subject line. Thank you.

© 2024 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at gibsondunn.com

U.S. Cybersecurity and Data Privacy Review and Outlook – 2024

Client Alert | January 29, 2024

I. Introduction In contrast to previous years, the 2023 privacy and cybersecurity landscape in the United States was not shaped by an overarching event like the COVID-19 pandemic or Russia’s invasion of Ukraine. 2023 was nonetheless another groundbreaking year for privacy and cybersecurity on the regulatory and enforcement fronts. Congress’s failure to pass a comprehensive privacy bill left the White House and federal agencies—along with state legislators and agencies—to lead the charge in regulating privacy and cybersecurity in the United States. The White House doubled down on its push to implement a national strategy on cybersecurity, with important implications for federal, state, and private entities. Numerous federal agencies—including the FTC, SEC, CFPB, and HHS—promulgated privacy and data protection regulations and guidance on a range of issues, including cyber-incident disclosure, children’s online privacy, biometric and genetic data, artificial intelligence (“AI”), and algorithmic decision making. Many agencies also brought enforcement actions against companies and (increasingly) individuals for privacy, data security, and related violations. States were similarly active in 2023, passing and enforcing a flurry of new comprehensive state privacy laws. State agencies like the New York Department of Financial Services took aggressive steps to tighten data protection regulations for entities under their umbrella. And, while this publication does not focus on AI (a topic which will be covered in detail by Gibson Dunn’s forthcoming Artificial Intelligence Legal Review), the rapid rise and proliferation of AI technology was a defining feature of the privacy and cybersecurity landscape in 2023. Litigation likewise remained active, with notable upticks in claims by private litigants and government entities related to data breaches, federal and state wiretapping laws, and state biometrics laws. We expect these trends to accelerate in 2024 and beyond, as the body of privacy and cybersecurity regulation matures and expands. This Review contextualizes these and other 2023 developments by addressing: (1) the regulation of privacy and data security, other legislative developments, enforcement actions by federal and state authorities, and new regulatory guidance; (2) trends in civil litigation around data privacy and security in areas including data breach, digital, telecommunications, wiretapping, and biometric information privacy laws; and (3) trends related to data innovations and governmental data collection. Information on developments outside the United States—which are relevant to domestic and international companies alike—will be covered in detail by Gibson Dunn’s forthcoming International Cybersecurity and Data Privacy Outlook and Review. **Table of Contents**

[I. INTRODUCTION](#)

[II. REGULATION OF PRIVACY AND DATA SECURITY](#)

[A. Regulation of Privacy and Data Security](#)

[1. State Legislation and Related Regulations](#)

[a. Comprehensive State Privacy Laws](#)

[i. Applicability](#) [ii. Exemptions](#) [iii. Data Subject Rights](#) [iv. Data Controller Obligations](#) [v. Enforcement](#)

Related People

[Cassandra L. Gaedt-Sheckter](#)

[Natalie J. Hausknecht](#)

[Martie Kutscher Clark](#)

[Timothy W. Loose](#)

[Abbey A. Barrera](#)

[Jacob U. Arber](#)

[Tony Bedel](#)

[Matt Buongiorno](#)

[Jay Mitchell](#)

[Wesley Sze](#)

[Terry Wong](#)

[Michael Brandon](#)

[Lane Corrigan](#)

[Justine Deitz](#)

[Skylar Drefcinski](#)

[Sasha Dudding](#)

[Erin Kim](#)

[Ruby B. Lang](#)

[Ignacio Martinez Castellanos](#)

[Peter Moon](#)

[Mason W. Pazhwak](#)

[Matthew C. Reagan](#)

[John Ryan](#)

[Becca Smith](#)

[Snezhana Stadnik Tapia](#)

[Graham M. Stinnett](#)

GIBSON DUNN

[b. Other State Privacy Laws](#)

[i. Washington's My Health My Data Act](#) [ii. Montana's Genetic Information Privacy Act](#)
[iii. California's Delete Act](#) [iv. New York Department of Financial Services' Amendments to Part 500 Cybersecurity Rules](#) [v. New Child Social Media Laws](#)

[2. Federal Legislation](#)

[a. Comprehensive Federal Privacy Legislation](#) [b. Other Introduced Legislation](#)

[B. Enforcement and Guidance](#)

[1. Federal Trade Commission](#)

[a. FTC Organization Updates](#) [b. Algorithmic Bias and Artificial Intelligence](#) [c. Commercial Surveillance and Data Security](#)

[i. FTC's Approach to Data Security](#) [ii. Rulemaking on Commercial Surveillance and Data Security](#)

[d. Notable FTC Enforcement Actions](#) [e. Financial Privacy](#) [f. Children's and Teens' Privacy](#) [g. Biometric Information](#)

[2. Consumer Financial Protection Bureau](#)

[a. Personal Financial Data Rights Rulemaking](#) [b. Increased Oversight of Non-bank Entities](#)
[c. Increased Scrutiny of Data Brokers](#) [d. Artificial Intelligence and Algorithmic Bias](#)

[3. Securities and Exchange Commission](#)

[a. Regulation](#) [b. Enforcement](#)

[4. Department of Health and Human Services and HIPAA](#)

[a. Rulemaking on HIPAA Compliance and Data Breaches](#) [b. Telehealth and Data Security Guidance](#)
[c. Reproductive and Sexual Health Data](#) [d. HHS Enforcement Actions](#)

[5. Other Federal Agencies](#)

[a. Department of Homeland Security](#) [b. Department of Justice](#) [c. Department of Commerce](#)
[d. Department of Energy](#) [e. Department of Defense](#) [f. Federal Communications Commission](#)

[6. State Agencies](#)

[a. California](#) [b. Other State Agencies](#) [c. Major Data Breach Settlements](#)

[III. CIVIL LITIGATION REGARDING PRIVACY AND DATA SECURITY](#)

[A. Data Breach Litigation](#)

[1. The Impact of *TransUnion v. Ramirez* on Standing in Data Breach Actions](#) [2. Cybersecurity Related Securities Litigation](#)

[B. Wiretapping and Related Litigation Concerning Online "Tracking" Technologies](#) [C. Anti-Hacking and Computer Intrusion Statutes](#)

[1. CFAA](#) [2. CDAFA](#)

[Cydney L. Swain](#)

[Julie Sweeney](#)

[Trenton J. Van Oss](#)

[Hayato Watanabe](#)

[Diego Wright](#)

[Samantha P. Yi](#)

GIBSON DUNN

[D. Telephone Consumer Protection Act Litigation](#) [E. State Law Litigation](#)

[1. California Consumer Privacy Act Litigation](#)

[a. Potential Anchoring Effect of CCPA Statutory Damages](#) [b. Requirements for Adequately Stating a CCPA Claim](#) [c. CCPA Violations Under the UCL](#) [d. The CCPA's 30-Day Notice Requirement](#) [e. Guidance on Reasonable Security Measures in Connection with the CCPA](#)

[2. State Biometric Information Litigation](#)

[a. Illinois Biometric Information Privacy Act](#)

[i. Expansion of BIPA's Scope](#) [ii. New Recognized Limitations Under BIPA](#)

[b. Texas Biometric Privacy Law Litigation](#) [c. New York Biometric Privacy Law Litigation](#)

[F. Other Noteworthy Litigation](#)

[IV. TRENDS RELATED TO DATA INNOVATIONS AND GOVERNMENTAL DATA COLLECTION](#)

[A. Data-Intensive Technologies—Privacy Implications and Trends](#) [B. Emerging Privacy Enhancing Technologies \(PETs\)](#) [C. Governmental Data Collection](#)

[V. CONCLUSION](#)

II. Regulation of Privacy and Data Security Since 2018, 14 states have enacted comprehensive data privacy legislation. Five of these are currently effective, and the remaining nine will go into effect between 2024 and 2026. A number of additional state legislatures considered comprehensive consumer privacy laws this past year but have yet to enact them. In addition, several states have passed narrower data privacy laws governing the use of specific categories of information, such as health and genetic information. These laws demonstrate the states' efforts to ensure the protection of consumers' data in the absence of a comprehensive federal data privacy law. We highlight several of these state privacy laws below and provide an overview of key similarities and differences.

A. Regulation of Privacy and Data Security

1. State Legislation and Related Regulations

a. Comprehensive State Privacy Laws

California was the first state to adopt a comprehensive data privacy law with the enactment of the California Consumer Privacy Act ("CCPA") in 2018. The California Privacy Rights Act ("CPRA") amended the CCPA in 2020. Since then, 13 other states—Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Montana, New Jersey, Oregon, Tennessee, Texas, Utah, and Virginia—have followed California in enacting comprehensive privacy laws. As shown in the below list of comprehensive state privacy laws enacted to date, five went into effect in 2023, an additional four will go into effect in 2024, four in 2025, and one in 2026. Most of these generally align with the standard template created by the comprehensive state privacy laws in Virginia, Colorado, Connecticut, and Utah, with a few having unique features, which are highlighted below. Please see [last year's Review](#) for a more detailed assessment of the comprehensive data privacy laws in California, Virginia, Colorado, Connecticut, and Utah, which have all now gone into effect. *Table 1: Comprehensive State Privacy Laws*

Law	Enacted Date
California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights	CCPA: June 28, 2018 CPRA: November 3, 2020

Act (CPRA) [1]	
Virginia Consumer Data Protection Act (VCDPA) [2]	March 2, 2021
Colorado Privacy Act (CPA) [3]	July 7, 2021
Connecticut Data Privacy Act (CTDPA) [4]	May 10, 2022
Utah Consumer Privacy Act (UCPA) [5]	March 24, 2022
Florida Digital Bill of Rights (FDBR) [6]	June 6, 2023
Texas Data Privacy and Security Act (TDPSA) [7]	June 18, 2023
Oregon Consumer Privacy Act (OCPA) [8]	July 18, 2023
Montana Consumer Data Privacy Act (MTCDDPA) [9]	May 19, 2023
Iowa Consumer Data Protection Act (ICDPA) [10]	March 29, 2023
Delaware Personal Data Privacy Act (DPDPA) [11]	September 11, 2023
New Jersey Data Privacy Act (NJDDPA) [12]	January 16, 2024
Tennessee Information Protection Act (TIPA) [13]	May 11, 2023
Indiana Consumer Data Protection Act (INCDPA) [14]	May 1, 2023

The tables below review core aspects of these laws, including applicability, exemptions, data subject rights, data controller obligations, and enforcement. **i. Applicability** Each comprehensive state privacy law applies to entities that conduct business in that state or provide products and services to residents of that state, and that meet certain applicability thresholds. As shown in Table 2 below, these thresholds typically relate to a company's annual gross revenue and/or the number of individuals whose personal information the business processes or controls. California is unique in applying its comprehensive privacy law to companies that derive 50% or more of their revenue from selling California residents' personal information, without pairing that requirement with a minimum number of consumers whose data is processed. Florida and Texas also have distinct requirements: Florida's statutory thresholds are designed to limit the application of the law to large companies, and Texas's law does not carry any fixed numerical thresholds with respect to gross revenue or number of consumers' whose data is processed. Unless otherwise indicated, all thresholds listed below are disjunctive requirements. *Table 2: Applicability of Comprehensive State Privacy*

Laws

Law	Annual Gross Revenue	Annual Processing of Consumers' Data	Other T
CCPA/CPRA (California)	\$25 million or more.	Buys, sells, or shares the personal information of 100,000 or more California residents, households, or devices.	Derives 50% or more revenue from California residents' per
VCDPA (Virginia)	N/A	Controls or processes the personal data of at least 100,000 Virginia consumers.	Controls or proce data of at least 100,000 Virginia consumers and derives c revenue from t
CPA (Colorado)	N/A	Processes the personal data of more than 100,000 Colorado individuals.	Derives reve discounts on g exchange for t data of 25,000
CTDPA (Connecticut)	N/A	Controls or processes the personal data of at least 100,000 Connecticut consumers.	Controls or proce data of at least 100,000 Connecticut consumers and derives c revenue from t info
UCPA (Utah)	\$25 million or more.	Controls or processes the personal data of 100,000 or more Utah consumers.	Controls or proce data of 25,000 or more Utah consumers and c of gross annual

			perso
FDBR (Florida)	\$1 billion or more.	N/A	(i) Derives 50% annual revenue from advertising or the (ii) operates a speaker and voice with an integrated through a cloud free verbal activation an app store to 250,000 software consumers
TDPSA (Texas)	N/A	N/A	(i) Conducts business produces products consumed by retail processes or entities personal data qualify as a small by the United States Administrat except
OCPA (Oregon)	N/A	Controls or processes the personal data of 100,000 or more Oregon consumers, other than for completing a payment transaction.	Controls or processes data of 25,000 consumers and of gross revenue perso
MTCDPA (Montana)	N/A	Controls or processes the personal data of 50,000 or more Montana consumers, excluding for the purpose of completing payment transactions.	Controls or processes data of 25,000 consumers and 25% of gross revenue perso
ICDPA (Iowa)	N/A	Controls or processes the personal data of 100,000 or more Iowa consumers.	Controls or processes data of 25,000 consumers and

			50% of gross re of pers
DPDPA (Delaware)	N/A	Controls or processes the personal data of at least 35,000 Delaware residents, excluding for the purpose of completing payment transactions.	Controls or pro data of at leas residents and de of its gross reve perso
NJDPA (New Jersey)	N/A	Controls or processes the personal data of at least 100,000 New Jersey consumers.	Controls or pro least 25,000 New and derives rev financial benefit
TIPA (Tennessee)	\$25 million or more.	Controls or processes the personal data of 170,000 or more Tennessee consumers.	Controls or pro data of 25,000 consumers and 50% of gross re personal
INCDPA (Indiana)	N/A	Controls or processes the personal data of 100,000 or more Indiana residents.	Controls or pro data of 25,00 consumers wh derives more revenue from t

ii. Exemptions All comprehensive state privacy laws also have exemptions for certain entities and categories of data. For example, non-profit entities and entities subject to the GLBA are exempt under most comprehensive state privacy laws. HIPAA-regulated data (but not necessarily entities regulated by HIPAA generally), employee data, and business contact data are likewise typically exempt under all comprehensive state privacy laws, except for in California. California is the only state whose GLBA exemption applies only at the data level, but not the entity level. Other exemptions not included below might include entities or data regulated by other laws, such as the Fair Credit Reporting Act, Driver’s Privacy Protection Act, Children’s Online Privacy Protection Act, the Family Educational Rights and Privacy Act, the Farm Credit Act, and the Airline Deregulation Act. Table 3 below provides a non-exhaustive list of common exemptions. *Table 3: Exemptions in Comprehensive State Privacy Laws*

Law	Non-Profits (generally)	Consumers Engaged in a Commercial or Employment	HIPAA the d le
------------	------------------------------------	--	-------------------------------

			Context (i.e., employees and business contacts)	
CCPA/CPRA (California)	N		N	
VCDPA (Virginia)	N		Y	
CPA (Colorado)	Y		Y	
CTDPA (Connecticut)	N		Y	
UCPA (Utah)	N		Y	
FDBR (Florida)	N		Y	
TDPSA (Texas)	N		Y	
OCPA (Oregon)	Y		Y	
MTCDDPA (Montana)	N		Y	
ICDDPA (Iowa)	N		Y	
DPDDPA (Delaware)	Y		Y	
NJDPA (New Jersey)	N		Y	
TIPA (Tennessee)	N		Y	
INDDPA (Indiana)	N		Y	

iii. Data Subject Rights All comprehensive state privacy laws that have been enacted or are in effect provide consumers with the right to access their data, data portability, opt-out of the sale of their data and use of certain data in connection with targeted advertising, and the right to not be discriminated against for exercising their rights. They also provide covered entities with the ability to verify or authenticate the identity of a consumer looking to exercise her rights. However, there are additional rights that are provided by some, but not all, comprehensive state privacy laws. These are outlined in Table 4 below. *Table 4: Data Subject Rights in Comprehensive State Privacy Laws*

Law	Correct Inaccurate Data	Request a List of Third Parties with Whom Data Has	Opt-Out of the Use of Data for Certain Profiling	Limit the Use and Disclosure of Sensitive Data	Appeal the Denial of Data Subject Rights Requests	

		Been Disclosed				R
CCPA/CPRA (California)	Y	N	Y	Limit use	N	
VCDPA (Virginia)	Y	N	Y	Opt-in	Y	
CPA (Colorado)	Y	N	Y	Opt-in	Y	
CTDPA (Connecticut)	Y	N	Y	Opt-in	Y	
UCPA (Utah)	N	N	N	Opt-out	N	
FDBR (Florida)	Y	N	Y	Opt-in	Y	
TDPSA (Texas)	Y	N	Y	Opt-in	Y	
OCPA (Oregon)	Y	Y	Y	Opt-in	Y	
MTCDDPA (Montana)	Y	N	Y	Opt-in	Y	
ICDDPA (Iowa)	N	N	N	Opt-out	Y	
DPDDPA (Delaware)	Y	N	Y	Opt-in	Y	
NJDPA (New Jersey)	Y	N	Y	Opt-in ^[15]	Y	
TIPA (Tennessee)	Y	N	Y	Opt-in	Y	

INCDPA (Indiana)	Y	N	Y	Opt-in	Y	
-----------------------------	---	---	---	--------	---	--

iv. Data Controller Obligations All comprehensive state privacy laws impose certain obligations on data controllers (entities that determine the purposes and means of processing of personal data). These include: data minimization; purpose limitations; maintaining privacy policies; maintaining reasonable administrative, technical, and physical data security controls; and contractually obligating personal data processors or service providers to comply with the applicable law. Data minimization in particular may be a significant requirement, as it requires companies to only keep data as long as they have a business need and promptly delete it thereafter. Some of the privacy laws impose additional obligations, which are outlined in Table 5 below. Specifically, some laws require (a) data protection impact assessments, which are designed to identify and minimize data protection risks, (b) financial incentive notices, which disclose discounts or other incentives that are provided in exchange for providing personal information, and (c) specific contractual requirements that set forth how vendors that process data on a business's behalf will act. *Table 5: Data Controller Obligations in Comprehensive State Privacy Laws*

Law	Data Prot Ass
CCPA/CPRA (California)	Y (no
VCDPA (Virginia)	
CPA (Colorado)	
CTDPA (Connecticut)	
UCPA (Utah)	
FDBR (Florida)	
TDPSA (Texas)	
OCPA (Oregon)	
MTCDPA (Montana)	
ICDPA (Iowa)	
DPDPA (Delaware)	
NJDPA (New Jersey)	
TIPA (Tennessee)	
INCDPA (Indiana)	

v. Enforcement Finally, there are differences between how each of these comprehensive state privacy laws are enforced and the penalties for noncompliance. As a general matter, comprehensive state privacy laws provide state attorneys general with sole enforcement authority. To date, the state laws have notably not provided for a private right of action. The only outlier is the CCPA/CPRA, which provides a limited private right of action for consumers affected by data breaches, under certain circumstances. Many states also provide for a right to cure, meaning that a plaintiff must provide a putative defendant with notice and an opportunity to cure the violation prior to bringing suit. The enforcement

mechanisms provided for by each comprehensive state privacy law are outlined in Table 6 below. *Table 6: Enforcement of Comprehensive State Privacy Laws*

Law	Private Right of Action	Enforcement Authority
CCPA/CPRA (California)	Y ^[16]	California Attorney General and California Privacy Protection Agency
VCDPA (Virginia)	N	Virginia Attorney General
CPA (Colorado)	N	Colorado Attorney General and district attorney
CTDPA (Connecticut)	N	Connecticut Attorney General
UCPA (Utah)	N	Utah Attorney General and Utah Division of Consumer Protection
FDBR (Florida)	N	Florida Department of Legal Affairs

TDPSA (Texas)		N	Texas Attorney General
OCPA (Oregon)		N	Oregon Attorney General
MTCDPA (Montana)		N	Montana Attorney General
ICDPA (Iowa)		N	Iowa Attorney General
DPDPA (Delaware)		N	Delaware Department of Justice
NJDPA (New Jersey)		N	New Jersey Attorney General
TIPA (Tennessee)		N	Tennessee Attorney General
INCDPA (Indiana)		N	Indiana Attorney General

b. Other State

Privacy Laws In addition to the comprehensive state privacy laws discussed above, states have continued to legislate in narrower areas, particularly with relation to health or genetic information. **i. Washington’s My Health My Data Act** On April 27, 2023, Washington Governor Jay Inslee signed the “My Health My Data Act” (“MHMDA”) into law, modifying the legal landscape with respect to health-related data for certain Washington entities.^[17] The MHMDA creates a privacy regime focused on personal health data. **Covered Entities.** The MHMDA applies to “regulated entities” that process “consumer health data.” The law defines “regulated entity” as any “legal entity” that: (1) “[c]onducts business in Washington or produces or provides products or services that are targeted to consumers in Washington”; and (2) “determines the purpose and means of collecting, processing, sharing, or selling of consumer health data,” whether “alone or jointly with others.”^[18] Practically, the law applies to any entity that does business in Washington and collects or processes consumer health data. Government agencies, tribal nations, and service providers that are contracted to process consumer health data on behalf of a government agency are exempt from this definition and not considered regulated entities.^[19] “Small businesses” are not exempt from the MHMDA, but are given an extra three months to comply.^[20] **Covered Data.** The law defines “consumer health data” as “personal information that is linked or reasonably linkable to a consumer and that identifies the consumer’s past, present, or future physical or mental health status.”^[21] Examples of this type of data include surgeries or other health-related procedures, reproductive or sexual health information, and genetic data.^[22] The primary statutory

carveout from the definition of “consumer health data” is information “used to engage in public or peer-reviewed scientific, historical, or statistical research.”^[23] However, the research must be monitored by an independent oversight entity that implements safeguards to mitigate privacy risks, including the risk associated with the reidentification of consumer data.^[24] The Washington Attorney General, who is charged with enforcing the MHMDA, has explained that purchases of “toiletry products (such as deodorant, mouthwash, and toilet paper)” do not qualify as “consumer health data,” even though they relate to “bodily functions,” whereas “an app that tracks someone’s digestion or perspiration is collecting consumer health data.”^[25] **Key Requirements.** The MHMDA prohibits regulated entities from collecting or sharing consumer health data without first satisfying certain notice and consent requirements, including: requiring regulated entities to maintain a “consumer health data privacy policy” linked to on their homepage that discloses:

- the categories of consumer health data collected and the purpose for which the data is collected;
- the categories of sources from which the consumer health data is collected;
- the categories of consumer health data shared; and
- a list of the categories of third parties and specific affiliates with whom the regulated entity shares the consumer health data.^[26]

Regulated entities may only collect or share consumer health data if a consumer provides a prior “clear affirmative act” expressing consent, or if the collection is “necessary to provide a product or service that the consumer . . . has requested.”^[27] **Consumer Rights.** The MHMDA also provides consumers with a number of protections, including the right to: (1) confirm whether a regulated entity is collecting, sharing, or selling their consumer health data; (2) access that data; (3) withdraw consent for the collection and sharing of their consumer health data; and (4) delete their data.^[28] **Enforcement.** A violation of the MHMDA is considered a violation of the Washington Consumer Protection Act.^[29] The Washington Attorney General may enforce the law.^[30] Consumers may also pursue private actions for violations of the MHMDA.^[31] **ii. Montana’s Genetic Information Privacy Act** On June 7, 2023, Montana Governor Greg Gianforte signed into law the “Montana Genetic Information Privacy Act” (“MTGIPA”). The MTGIPA applies to any entity that offers consumer genetic testing products or services directly to a consumer, or collects, uses, or analyzes genetic data.^[32] “Genetic data” is defined as “any data, regardless of format, concerning a consumer’s genetic characteristics.”^[33] The MTGIPA requires covered entities to provide a privacy policy and notice regarding their use of genetic data and to obtain a consumer’s “express consent” in order to collect, use, or disclose a consumer’s genetic data.^[34] The MTGIPA also requires an entity to “develop, implement, and maintain a comprehensive security program to protect a consumer’s genetic data against unauthorized access, use, or disclosure.”^[35] The Montana Attorney General has sole authority to enforce the MTGIPA.^[36] **iii. California’s Delete Act** On October 10, 2023, California Governor Gavin Newsom signed the “Delete Act” into law.^[37] The law revises California’s data broker registration law and gives consumers the right to manage data held by data brokers free of charge by submitting a single deletion request to a centralized website.^[38] After a deletion request is submitted, a data broker is required to delete data within 45 days, and continue deleting any personal information collected about that consumer at least every 45 days thereafter.^[39] After a consumer has submitted a deletion request, data brokers are also prohibited from selling or sharing new personal information about the consumer in the future.^[40] Consumers will have the option to “selectively exclude” data brokers when submitting a deletion request.^[41] The law also requires data brokers to “undergo an audit by an independent third party to determine compliance” with the law.^[42] Under the law, a “data broker” is defined as “a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship.”^[43] But the law includes exemptions for entities covered by the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, the Insurance Information and Privacy Protection Act, the Confidentiality of Medical

Information Act, or HIPAA, and business associates of covered entities under the Confidentiality of Medical Information Act or HIPAA.^[44]

iv. New York Department of Financial Services' Amendments to Part 500 Cybersecurity Rules On November 1, 2023, the New York State Department of Financial Services ("NYDFS") issued its Second Amendment to 23 NYCRR Part 500 ("Part 500"), which establishes numerous cybersecurity requirements for regulated entities.^[45] As discussed in more depth in our recent [client alert](#), the amendments to Part 500 include: expanded responsibility for senior governing bodies, obligations to implement additional safeguards, new requirements for larger companies, new and increased obligations related to written policies and procedures, heightened requirements around audits and risk assessments, and additional reporting requirements for cybersecurity incidents. NYDFS is responsible for enforcing Part 500 and has brought several enforcement actions against various financial entities, including banks, money transfer service providers, and cryptocurrency service providers.^[46]

v. New Child Social Media Laws Several states passed laws restricting social media apps, but those laws have been challenged in the courts. For example, Utah's Social Media Regulation Act^[47] requires social media companies with at least 5,000,000 account holders worldwide to verify the age of adults seeking to maintain or open social media accounts; obtain parental consent for users under the age of 18 to open an account; imposes restrictions on children's accounts; and prohibits collections of certain data and targeted advertising.^[48] The law may be enforced by either the Division of Consumer Protection or through a private right of action.^[49] Plaintiffs may obtain up to \$2,500 in statutory damages per violation, in addition to attorney's fees and costs.^[50] The law has been challenged in two different suits that are ongoing.^[51] A similar law in Arkansas that would require parental permission for children to create certain social media accounts was blocked by a federal judge.^[52] The judge concluded in granting the preliminary injunction that the law, as written, was unconstitutionally vague because it failed to adequately define "social media company," and therefore which entities were subject to its requirements.^[53] The judge also agreed that the law likely violates the First Amendment because the age verification process would chill speech by deterring adults from signing up for social media accounts and that the law is unnecessarily overbroad insofar as it attempts to protect minors from harmful or obscene content.^[54] And a Montana federal judge blocked a law in that state that would prohibit mobile application stores from offering TikTok to Montana users.^[55] The court, in granting the preliminary injunction, found that plaintiffs were likely to succeed on the merits of their arguments—namely, that an outright ban on a specific app likely violates the First Amendment, the Commerce Clause, and is preempted by federal national security law, among other reasons.^[56]

2. Federal Legislation

a. Comprehensive Federal Privacy Legislation Comprehensive federal privacy legislation remains a popular, yet unrealized, objective despite recent congressional efforts. The American Data Privacy and Protection Act ("ADPPA") introduced in 2022 was the most advanced attempt to-date at enacting a comprehensive federal privacy bill. However, the bill died when it failed to advance to the House or Senate floors before the last Congress adjourned in January 2023.^[57] As proposed, the ADPPA bill required covered companies to engage in "data minimization" and adopt "privacy by design" principles.^[58] The ADPPA also prohibited covered entities from designing and employing discriminatory algorithms, and required them to study the impacts of their algorithms.^[59] Government enforcement of the ADPPA would have been left largely to the FTC at the federal level, alongside state attorneys general and other key state officials.^[60] But the ADPPA's addition of a private right of action was a source for serious concern due to the burden and cost of class action lawsuits.^[61] The bill also explicitly preempted most state privacy laws—a fact that some believe was largely responsible for the bill's demise.^[62] Calls for comprehensive federal privacy legislation continued throughout 2023 despite the ADPPA's failure. In the spring, Congress held hearings on the continuing need for such legislation.^[63] President Biden echoed these calls in an executive order (which also enacted AI safety measures).^[64] In his 2023 State of the Union address, the President likewise called for stronger online privacy protections for children.^[65]

b. Other Introduced Legislation Congress did not pass any privacy laws in 2023, although a significant number of consumer and individual privacy-related legislation was introduced.^[66] This proposed privacy legislation covered a range of topics, including surveillance technologies, health privacy, privacy for children online, facial

recognition, AI, and cybersecurity. Many of the measures attracted significant bipartisan support, but lawmakers remained divided over the same two issues that sunk more comprehensive federal privacy legislation: (1) whether federal privacy laws should preempt state laws (a position attracting more Republican support) and (2) whether it should include a private right of action (which more Democrats favor). Nevertheless, in the absence of comprehensive federal privacy legislation, Congress may still be more likely to enact legislation on a narrower topic that draws more bipartisan support, such as children’s online safety, in the future.^[67] Lawmakers focused in particular on digital privacy and safety in 2023, especially for children on social media. They held widely publicized hearings on the topic, bringing in social media executives for questioning, with more hearings to come in 2024.^[68] In July 2023, the U.S. Senate Commerce Committee advanced a pair of measures seeking to put more responsibility on social media platforms to ensure child safety online: the Kids Online Safety Act, which would require platforms to enact measures to prevent harms to minors and to restrict targeted advertising for children under 13;^[69] and COPPA 2.0, which would upgrade and expand the original children’s online privacy law, including by adding protections for teens ages 13 to 16.^[70] Other privacy bills introduced in 2023 include: the Informing Consumers about Smart Devices Act (requiring manufacturers to disclose that a camera or microphone is part of a device before purchase),^[71] the Stop Spying Bosses Act (requiring disclosure of or prohibiting surveillance, monitoring, and collection of worker data),^[72] the UPHOLD Privacy Act (establishing protection for personally identifiable health and location data),^[73] the DELETE Act (requiring the FTC to establish a system allowing individuals to request that data brokers delete their personal information),^[74] the Data Care Act of 2023 (imposing duty of care, loyalty, and confidentiality on online service providers),^[75] the Online Privacy Act of 2023 (establishing individual privacy rights and creating a private right of action and Digital Privacy Agency),^[76] and others described in this Review. Congress also considered cybersecurity-related legislation: the Federal Cybersecurity Vulnerability Reduction Act of 2023 (requiring certain government contractors to adopt vulnerability disclosure policies),^[77] the Modernizing the Acquisition of Cybersecurity Experts Act of 2023 (generally barring agencies from setting minimum educational requirements for cybersecurity workers),^[78] and the Federal Cybersecurity Workforce Expansion Act (providing training and apprenticeships for cybersecurity workers).^[79]

B. Enforcement and Guidance In 2023, government regulators remained active in enforcement and regulatory efforts related to data privacy, cybersecurity, and new technology. This section summarizes notable regulatory and enforcement efforts by the Federal Trade Commission (“FTC”), Consumer Financial Protection Bureau (“CFBP”), Securities and Exchange Commission (“SEC”), Department of Health and Human Services (“HHS”), and other federal and state agencies.

1. Federal Trade Commission The FTC remained active in the regulation and enforcement of cybersecurity and data privacy in 2023—and continued to aggressively pursue new regulatory, enforcement, and litigation matters in other areas as well. Several actions, such as its rulemaking on junk fees, have had important impacts on online businesses. For example, the proposed junk fees rule was introduced in direct response to President Biden’s announced priorities for consumer protection’ and following his call for transparency in consumer pricing.^[80] The FTC extended the comment period for the rule through February 7, 2024.^[81] As currently drafted, the rule would ban “hidden fees”—or fees that are mandatory, even if provided by a different entity. It would also ban “misleading fees,” essentially requiring disclosure of the purpose and refundability of any fees charged. The FTC also continued to prioritize algorithmic bias and AI, commercial surveillance, data security, and children’s privacy. Further, the FTC expanded its regulatory and enforcement scope related to biometric information. This section discusses the FTC’s notable actions on these topics in 2023.

a. FTC Organization Updates In March 2023, Republican Commissioner Christine Wilson resigned abruptly from the FTC, publicly citing her disagreements with Chair Lina Khan’s vision and management of the FTC.^[82] This created an additional vacancy on the five-member commission, following the departure of Commissioner Noah Phillips in October 2022. In July 2023, President Joe Biden nominated two Republican replacements: Virginia Solicitor General Andrew Ferguson and Utah Solicitor General Melissa Holyoak.^[83] Prior to his current appointment as Virginia Solicitor General, Ferguson served in numerous roles on the Hill, including as Chief Counsel to Senate Minority Leader Mitch McConnell, as Chief

Counsel for Nominations and the Constitution to then-Judiciary Committee Chairman Lindsey Graham, and as Senior Special Counsel to then-Judiciary Committee Chairman Chuck Grassley. Holyoak previously served as President and General Counsel of a nonprofit public-interest law firm that advocates for free markets, free speech, and limited government. In their confirmation hearing, both Holyoak and Ferguson demonstrated interest in regulating big technology companies. Holyoak specifically called out the importance of protecting children online.^[84] Both nominations are currently held up in the Senate.^[85] If confirmed, the new Commissioners will not change the Republican-Democrat balance of power at the FTC, which has been led by a Democratic majority since Commissioner Bedoya was confirmed in 2022.

b. Algorithmic Bias and Artificial Intelligence The FTC continues to signal that AI and algorithms are an enforcement priority. In a mid-year public editorial, for instance, FTC Chair Lina Kahn warned of the risks AI poses, including producing discriminatory outcomes and potential privacy violations.^[86] As reflected in Chair Khan's editorial, the FTC is particularly concerned about the effects algorithms may have on consumer privacy, including the use of consumer data to train large language models and inadvertent disclosure of personally identifiable information ("PII") through chatbots. In a series of AI-focused blog posts published from February to August 2023, the FTC warned businesses that they should avoid using automated tools that result in biased or discriminatory impacts. One post further noted that businesses "can't just blame a third-party developer of the technology" when reasonably foreseeable failures occur; instead, businesses should investigate and identify the foreseeable risks and impact of AI before using it in a consumer-facing setting.^[87] In March 2023, the FTC also specifically called out AI technology that simulates human activity and can be used by third-party bad actors to, among other things, target communities of color with fraudulent schemes.^[88] It warned that businesses considering launching tools with such risks must employ deterrents that go beyond "bug corrections or optional features that third parties can undermine via modification or removal."^[89] Other use cases highlighted by the FTC as targets for enforcement include: technology that enables "deepfakes" and "voice cloning,"^[90] customizing ads to specific people or groups in a manner that "trick[s] people into making harmful choices[.]"^[91] and tools that purport to detect generative AI content.^[92] For a more detailed discussion of regulatory developments in AI, please see Gibson Dunn's forthcoming Artificial Intelligence Legal Review.

c. Commercial Surveillance and Data Security

i. FTC's Approach to Data Security In a February 2023 blog post, the FTC's Deputy Chief Technology Officer Alex Gaynor highlighted three best practices for effectively protecting user data drawn from recent FTC orders: (i) requiring multi-factor authentication (for consumers and employees); (ii) requiring a company's systems connections to be encrypted and authenticated; and (iii) requiring data retention schedules to be published and followed.^[93] Gaynor warns that these practices alone "are not the sum-total of everything the FTC expects from an effective security program."^[94] He nevertheless suggests a security program is highly likely to be effective if it incorporates these practices.^[95]

ii. Rulemaking on Commercial Surveillance and Data Security As described in Gibson Dunn's [prior alert](#), the FTC's Advance Notice of Proposed Rulemaking on commercial surveillance and data security would overhaul the regulatory landscape for corporate internet use. FTC Consumer Protection Chief Samuel Levine noted in a speech in September 2023 that the FTC is currently reviewing over 11,000 comments received in response to the request for comment, which closed on November 21, 2022.^[96] If adopted, the rule will have widespread impact, implicating every facet of the internet from advertising to algorithmic decision-making. The advanced notice for the proposed rule, for instance, seeks comment on issues as wide ranging as whether consumer consent is still an effective gatekeeper for corporate data practices, whether the FTC should forbid or limit the development, design, and use of certain automated decision-making systems, and whether the FTC should adopt workplace, teen, or industry-specific (e.g., health- or finance-related) rules around data collection and use. The FTC is expected to take final action on the proposed rule in 2024.^[97]

d. Notable FTC Enforcement Actions In 2023, the FTC maintained its aggressive stance on privacy enforcement, which has been a hallmark of Chair Khan's tenure. In addition to enforcement actions that hold companies responsible for the activities discussed, there has also been a rise in actions brought against individuals. Below we discuss some of the

FTC's most notable enforcement actions in 2023. **Video Game and Software Developer.** In March 2023, the FTC finalized an order in an action originally described in [last year's Review](#), which will require a large video game and software developer to pay \$245 million to refund affected consumers and bans the company from charging consumers through the use of "dark patterns" or otherwise charging consumers without obtaining their affirmative consent.[\[98\]](#) The order also bars the company from blocking consumers' access to their accounts if the consumer is disputing unauthorized charges. **Home Security Camera Company.** The FTC brought an action under Section 5(a) of the FTC Act,[\[99\]](#) challenging a security camera company's representations regarding security, and alleging that employees and contractors were able to access private videos.[\[100\]](#) A proposed settlement would require deletion of certain data and affected data products "such as data, models, and algorithms derived from videos it unlawfully reviewed," establishment of a privacy and data security program, obtaining assessments by a third party, and cooperation with a third-party assessor.[\[101\]](#) **Tax Preparation Firms.** The FTC issued Notices of Penalty Offenses to five tax preparation firms about the use of information collected for tax preparation services to solicit loan borrowers. A Notice of Penalty Offense is intended to put companies on notice of prior successful enforcement actions against other companies, but does not mean the FTC has found the recipients are violating the law.[\[102\]](#) However, the FTC's Notice warned that the companies could face civil penalties of up to \$50,120 per violation if they use or disclose consumer confidential data collected for tax preparation for other purportedly unrelated purposes, such as advertising, without express consumer consent.[\[103\]](#) **Voice Assistant.** In May, DOJ brought an action on behalf of the FTC against a major technology company that includes, among its products, a voice assistant.[\[104\]](#) The FTC alleged that the company improperly prevented parents from deleting their children's data and retained and risked exposure of sensitive data. The FTC's settlement with the company, approved in July 2023, requires the company to overhaul its deletion practices, as well as implement stronger privacy safeguards to settle Children's Online Privacy Protection Act Rule ("COPPA Rule") claims and deception claims about its data deletion practices.[\[105\]](#) **Telehealth and Prescription Drug Provider.** The FTC brought its first enforcement action under the Health Breach Notification Rule, which was originally adopted in 2009 and requires vendors of personal health records and related entities to notify consumers, the FTC, and, in some cases, the media, when such data is disclosed or acquired without consumers' authorization.[\[106\]](#) The FTC alleged that the company failed to notify consumers, the FTC, and the media about its disclosure of individually identifiable health information to certain online services. This enforcement action followed a 2021 FTC policy statement that purported to require health apps and other online services to comply with the Health Breach Notification Rule.[\[107\]](#) The company agreed to pay a \$1.5 million civil penalty and is barred from sharing user health data with third parties for advertising.[\[108\]](#) The FTC also proposed amendments to the Health Breach Notification Rule, with a public comment period that ended on August 8, 2023.[\[109\]](#) **Genetic Testing Firm.** The FTC settled allegations against a genetic testing firm for allegedly leaving user data unprotected, misleading users about their ability to delete their data, and retroactively changing its privacy policy without proper notice to consumers. In addition to monetary penalties of \$75,000, as part of the final order, the company is required to take remedial actions including instructing third-party contractors to destroy all DNA samples retained beyond a specified timeframe, notifying the FTC of any unauthorized disclosure of consumer personal health data, and implementing a comprehensive information security program.[\[110\]](#) **In-Store Surveillance and Facial Recognition.** For the first time, the FTC alleged that the use of facial recognition technology may be an unfair practice or deceptive under Section 5 of the FTC Act.[\[111\]](#) The FTC alleged that a national pharmacy chain deployed AI-facial recognition technology to identify shoplifters and other problematic shoppers. The FTC's complaint alleged that the company failed to take reasonable measures to prevent harm to consumers who were erroneously accused by employees of wrongdoing because the technology incorrectly flagged the consumers as matching the profile of a known shoplifter or troublemaker. The FTC banned the retailer's use of facial recognition technology for five years. While the FTC also alleged the company violated the terms of a 2010 consent decree by failing to comply with its own information security program's policies and contractual requirements for facial technology vendors, the FTC

did not seek civil penalties, and imposed a no-money, no-fault order. The case helpfully articulates what the FTC deems as “best practices” for the use of facial recognition technologies, including the usage of cameras and smartphones by retailers to detect and stop shoplifting and to mitigate risks of misidentification. **e. Financial Privacy** The FTC approved further changes to its Standards for Safeguarding Customer Information Rule (“Safeguards Rule”) in 2023. The Safeguards Rule requires non-banking financial institutions, such as mortgage brokers, motor vehicle dealers, and payday lenders, to develop, implement, and maintain a comprehensive security program to keep their customers’ information safe. The rule was initially amended in October 2021 in response to “widespread data breaches and cyberattacks” by introducing more robust data security requirements for financial institutions to protect their customers’ data.^[112] In 2023, the FTC further amended the rule to require financial institutions to report certain data breaches directly to the FTC.^[113] Many provisions of the 2021 rule changes went into effect on January 10, 2022, but certain provisions of the Safeguards Rule did not take effect until June 9, 2023.^[114] These sections require financial institutions to:

- Designate a qualified individual to oversee their information security program;
- Develop a written risk assessment;
- Limit and monitor who can access sensitive customer information;
- Encrypt all sensitive information;
- Train security personnel;
- Develop an incident response plan;
- Periodically assess the security practices of service providers; and
- Implement multifactor authentication or another method with equivalent protection for any individual accessing customer information.^[115]

The FTC’s 2023 amendments include more specific criteria for what safeguards financial institutions must implement as part of their information security program, and requirements to explain their information-sharing practices and designate a single qualified individual to oversee their information security program and report periodically to an organization’s board of directors, or a senior officer in charge of information security.^[116] These amendments will not take effect until mid-2024. **f. Children’s and Teens’ Privacy** On December 20, 2023, the FTC announced long-awaited proposed amendments to the Children’s Online Privacy Protection Rule (“COPPA Rule”).^[117] If adopted, the proposed amendments would be the first changes to the COPPA Rule in a decade.^[118] The amendments aim to modernize the COPPA framework and shift the burden for protecting children’s privacy and security from parents to service providers.^[119] The proposed changes include:

- Requiring separate opt-in for targeted advertising;
- Prohibiting conditioning a child’s participation on collection of personal information;
- Limiting the support for the internal operations exception, which allows operators to collect persistent identifiers without first obtaining verifiable parental consent as long as the operator does not collect any other personal information;
- Imposing restrictions on educational technology companies, including prohibiting these companies’ use of students’ data for commercial purposes;
- Increasing accountability for Safe Harbor programs, including by requiring each program to publicly disclose its membership list and report additional information to the Commission;
- Strengthening data security requirements; and
- Limiting data retention.^[120]

The FTC also recently sought comments from the Entertainment Software Rating Board and others for a new mechanism for obtaining parental consent under the COPPA Rule: “Privacy-Protective Facial Age Estimation” technology, which analyzes the geometry of a user’s face to accurately confirm a user’s age.^[121] The FTC’s request for comments focused on whether such age verification methods would satisfy the COPPA Rule’s requirements and whether it poses a privacy risk to children’s biometric and other personal information.^[122] In 2023, the FTC pursued enforcement action against major technology companies in relation to children’s and teen’s’ privacy. For example, the FTC alleged a technology company violated the COPPA Rule by collecting and illegally retaining personal information from children who signed up for a gaming service without parental consent.^[123] The company agreed to pay \$20 million and take steps to increase privacy protection for children users to settle the case.^[124] The FTC has also proposed changes to its 2020 order with another technology company, alleging in part that the company has not fully complied with the order because it misled parents about their ability to control with whom their children communicated.^[125] Among other things, the proposed changes would prohibit the company from monetizing data it collects from users under 18.^[126]

g. Biometric Information On May 18, 2022, the FTC signaled an increased focus on preventing the misuse of biometric information in a policy statement.^[127] The policy statement is a first-of-its-kind comprehensive breakdown of the FTC’s view that the commercial use of biometric information poses certain privacy risks to consumers, and it builds on prior workshops and statements analyzing consumer protection issues related to specific technologies that can implicate biometric information.^[128] In the policy statement, the FTC broadly defines biometric information as data depicting or describing a person’s physical, biological, or behavioral traits, characteristics, or measurements, including facial features, iris or retina, fingerprints or handprints, voice, genetics, or characteristic movements or gestures.^[129] The FTC warned that certain conduct relating to the use of biometric information and biometric information technologies constitutes an unfair or deceptive practice under Section 5 of the FTC Act, including:

- Making false or unsubstantiated marketing claims regarding the validity, reliability, accuracy, performance, fairness, or efficacy of technologies relying on biometric information;
- Making deceptive statements about the collection and use of biometric information;
- Failing to protect consumers’ biometric information using reasonable data security practices;
- Collecting biometric information that consumers meant to conceal or keep private (including by implementing “privacy-invasive default settings”);
- Selling technologies that permit harmful or illegal conduct, such as covert tracking; and
- Using or selling discriminatory technologies.^[130]

To avoid liability under the FTC Act, the FTC recommends that businesses communicate the use and capabilities of biometric information technologies to consumers, ensure biometric information technologies operate fairly and accurately, and implement safeguards to prevent unauthorized access to biometric information. Relying on the policy statement for the first time, the FTC filed a complaint in December 2023 alleging that a drugstore chain surreptitiously used facial recognition technology to identify—sometimes falsely—shoplifters and other customers it deemed problematic, as described above.^[131]

2. Consumer Financial Protection Bureau Notwithstanding increasing congressional antagonism directed at the Consumer Financial Protection Bureau (“CFPB”), the CFPB did not decrease its attention on privacy issues in 2023. Last year, the CFPB issued a long-awaited proposed rule regarding consumer personal financial data rights and signaled an intent to increase its oversight of non-bank entities providing digital wallets and peer-to-peer apps, as well as data brokers that sell certain types of consumer data. The CFPB also parroted the FTC’s concerns with privacy risks associated with AI.

a. Personal Financial Data Rights Rulemaking On October 19, 2023, the CFPB released a long-

awaited Notice of Proposed Rulemaking on Personal Financial Data Rights.^[132] If adopted, this rule would establish a regulatory framework where consumers have the power “to break up with banks that provide bad service and would forbid companies that receive data from misusing or wrongfully monetizing the sensitive personal financial data.”^[133] The proposed rule would also require covered financial entities to share a consumer’s financial data with authorized third parties upon the consumer’s request.^[134] The proposed rule is the first proposal to implement Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (“Dodd-Frank Act”), which authorizes the CFPB to prescribe rules under which consumers may access information about themselves from their financial service providers.^[135] Although Section 1033 applies to all consumer financial products or services covered under the Dodd-Frank Act,^[136] the proposed rule would limit the scope of covered entities, or “data providers,” to Regulation Z card issuers, Regulation E financial institutions, and other payment facilitation providers, while generally exempting data providers that do not have a consumer interface.^[137] Under the proposed rule, data providers must provide consumers and authorized third parties with “covered data,” such as transaction information, account balance, and upcoming bill information, “in an electronic form usable by consumers and authorized third parties,” as provided by Section 1033 of the Dodd-Frank Act.^[138] In addition to requiring third parties to obtain “express informed consent” from the consumer to become authorized to access covered data, the proposed rule would also prohibit such authorized third parties from collecting, using, or retaining the consumer’s relevant data beyond what is “reasonably necessary” to provide the requested product or service to a consumer.^[139] The proposal does not define what is “reasonably necessary,” but instead enumerates activities that do not qualify: (i) targeted advertising; (ii) cross-selling of other products or services; or (iii) the sale of covered data.^[140] The proposed rule also imposes data accuracy and data security obligations, among other obligations, on authorized third parties.^[141] The comment period for the proposed rule closed on December 29, 2023; CFPB Director Rohit Chopra said that the agency intends to finalize the rule by fall 2024.^[142]

b. Increased Oversight of Non-bank Entities On November 7, 2023, the CFPB issued a proposed rule that, if adopted, would establish supervisory power over big technology firms and other nonbank entities that offer services allowing consumers to digitally transfer money.^[143] The proposed rule would apply to “larger participant” nonbank entities that handle more than five million payment transactions per year through digital wallets, peer-to-peer apps, payment apps, and other “covered payment functionalities.”^[144] This oversight authority would allow the CFPB to conduct examinations to ensure that these nonbank entities are adhering to applicable laws governing funds transfer, privacy, and consumer protection.^[145] The comment period for this proposed rule closed on January 8, 2024.^[146]

c. Increased Scrutiny of Data Brokers In March 2023, the CFPB launched an inquiry into data brokers to inform whether existing Fair Credit Reporting Act (“FCRA”) rules reflect the market realities of “[m]odern data surveillance practices [that] have allowed companies to hover over our digital lives and monetize our most sensitive data.”^[147] The agency’s request for information defined “data brokers” broadly as “an umbrella term to describe firms that collect, aggregate, sell, resell, license, or otherwise share consumers’ personal information with other parties.”^[148] That definition could sweep in companies, like credit unions and banks, that are not typically considered data brokers. On August 15, 2023, Director Chopra also announced that the CFPB will be developing new rules that define a data broker that sells certain types of consumer data as a “consumer reporting agency” (“CRA”) under FCRA.^[149] Defining data brokers as CRAs would impose new obligations on data brokers to comply with FCRA’s demanding standards for data accuracy and privacy, including consumer access and consent rights.^[150] Director Chopra also announced a second proposal under consideration that will clarify the extent to which credit header data, such as name, date of birth, and social security number, constitute a consumer report, and thereby limit the ability of CRAs to impermissibly disclose identifying contact information.^[151] The CFPB intends to propose these changes for public comment in 2024.^[152]

d. Artificial Intelligence and Algorithmic Bias In an April 25, 2023 joint statement with the DOJ, FTC, and Equal Employment Opportunity Commission, the CFPB reaffirmed its commitment to enforce consumer financial protection laws to prevent harmful uses of AI and algorithmic bias.^[153] Since then, the CFPB has highlighted risks

associated with AI in multiple contexts: **Chatbots**. In June 2023, the CFPB released an issue spotlight on the risks associated with the use of chatbots by financial institutions, including consumer financial protection compliance risks and failures to protect consumer privacy and data, diminished trust and customer service, and harm to consumers resulting from inaccurate information.[\[154\]](#) **Home Appraisals**. In June 2023, the CFPB also proposed a rule that would govern automated home valuations.[\[155\]](#) The rule would require institutions that employ automated valuation models to take certain steps to minimize inaccuracy and bias by adopting policies, practices, procedures, and control systems to ensure that models adhere to quality control standards designed to ensure a high level of confidence in the estimates produced.[\[156\]](#) Under the proposal, institutions would also be required to protect against the manipulation of data, seek to avoid conflicts of interest, require random sample testing and reviews, and comply with applicable nondiscrimination laws.[\[157\]](#) The public comment period ended on August 21, 2023.[\[158\]](#) **Credit Decisions**. In September 2023, the CFPB issued a Consumer Protection Circular titled “Adverse Action Notification Requirements and the Proper Use of the CFPB’s Sample Forms Provided in Regulation B,” concerning lenders’ obligations when using AI to make consumer credit decisions.[\[159\]](#) The guidance emphasizes that creditors must provide accurate and specific reasons for adverse decisions made by complex algorithms, and this requirement is not automatically satisfied by use of a sample adverse action checklist.[\[160\]](#) **3. Securities and Exchange Commission** In 2023, the SEC continued to focus on transparency around cybersecurity risk management and incident disclosure, as made evident by the Commission’s rulemaking and enforcement activity. Most notably, the SEC finalized rules requiring public companies to report material cybersecurity incidents within four business days of determining materiality, as well as periodic disclosures relating to cybersecurity risk management, strategy, and governance. The SEC was also active on the enforcement front, pursuing actions against companies and individuals in connection with cyber incidents. In 2024, we expect to see heightened enforcement activity as the newly adopted cyber rules take effect and as the SEC takes final action on proposed rulemaking for registered entities, particularly those implicating personal information or sensitive data. **a. Regulation March 2023 – SEC Proposes Rules to Amend Regulation S-P** On March 15, 2023, the SEC proposed rules that would amend Regulation S-P to update and close certain gaps in the requirements pertaining to the protection of customer information.[\[161\]](#) Most importantly, if adopted, the amendments would require broker-dealers, investment companies, registered investment advisers, and transfer agents (“Covered Institutions”) to adopt written policies and procedures for responding to unauthorized access to or use of customer information.[\[162\]](#) The amendments would also require Covered Institutions to notify individuals of unauthorized use of or access to their sensitive information “as soon as practicable,” but not later than 30 days, after discovery of a data breach.[\[163\]](#) As explained in the adopting release, the rules would also amend other aspects of Regulation S-P, including:

- Extending the protections of the safeguards and disposal rules to both nonpublic personal information that a Covered Institution collects about its own customers and to nonpublic personal information that a covered institution receives about customers of other financial institutions;
- Extending the safeguards rule, as amended, to registered transfer agents, and expanding the disposal rule to include transfer agents registered with another appropriate regulatory agency; and
- Conforming Regulation S-P’s existing provisions relating to the delivery of an annual privacy notice for consistency with a statutory exception created by Congress in 2015.[\[164\]](#)

The public comment period closed on June 5, 2023, but the SEC has not indicated whether and when it will take final action on the proposed amendments. **July 2023 – SEC Adopts New Cybersecurity Disclosure Rules for Public Companies** On July 26, 2023, as reported in Gibson Dunn’s [client alert](#), the SEC adopted a final rule to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incidents by public companies that are subject to the reporting requirements of the

SEC Act of 1934 (the “Exchange Act”).^[165] The final rule requires: (i) Form 8-K disclosure of material cybersecurity incidents within four business days of the company’s determination that the cybersecurity incident is material; and (ii) annual disclosures in Form 10-K regarding the company’s cybersecurity risk management, strategy, and governance.^[166] For foreign private issuers, the final rule amends Form 20-F to include requirements parallel to Item 106 regarding risk management, strategy, and governance.^[167] In addition, the final rule adds “material cybersecurity incidents” to the items that may trigger a current report on Form 6-K.^[168] Under the new rule, foreign private issuers will be required to furnish on Form 6-K information about material cybersecurity incidents that the issuers disclose or otherwise publicize in a foreign jurisdiction, to any stock exchange or to security holders.^[169] **Compliance Dates** The Form 8-K disclosure requirement went into effect on December 18, 2023 for most registrants (smaller companies will have until June 5, 2024 to comply); all registrants will have to comply with the annual disclosure requirements beginning with their Form 10-K or 20-F filing for the fiscal year ending on or after December 15, 2023.^[170] **Reporting Material Cybersecurity Incidents** Under the final rules, when a company experiences a material cybersecurity incident, it must disclose on Form 8-K, the material aspects of the nature, scope, and timing of the incident, and the material impact or “reasonably likely” material impact on the company, including on its financial condition and results of operations.^[171] Importantly, this disclosure must be made within four business days of the company determining that it has experienced a material cyber incident, a determination which must be made “without unreasonable delay after discovery of the incident.”^[172] In circumstances where a company has determined that a cybersecurity incident is material but does not have all of the information that is required to be disclosed when the Form 8-K filing is due, the company must later update the disclosure through a Form 8-K amendment.^[173] The final rule permits companies to delay reporting material cyber incidents up to an initial period of 30 days, if the U.S. Attorney General notifies the SEC in writing that immediate disclosure would pose a substantial risk to national security or public safety.^[174] However, as confirmed by guidelines released by the Department of Justice,^[175] the Attorney General will only permit delayed disclosures in very limited circumstances, so public companies should be prepared to disclose virtually all material cyber incidents within four days after determining materiality.^[176] The DOJ guidelines also make clear that even where the Attorney General grants a delay, the delay may not delay filing the Form 8-K in its entirety, but may only pertain to some of the information that is required to be disclosed.^[177] **Annual Reporting Requirements** The final rule also requires that public companies include on their Form 10-K filings certain disclosures regarding the company’s cybersecurity risk management, strategy and governance.^[178] The final rule also includes parallel requirements for a foreign private issuer’s risk management, strategy, and governance disclosures on Form 20-F.^[179] *Risk management strategy and governance disclosure.* Companies are required to describe their processes for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes, including information regarding:

- Whether and how any such processes have been integrated into the company’s overall risk management system or processes;
- Whether the company engages assessors, consultants, auditors, or other third parties in connection with any such processes; and
- Whether the company has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider.^[180]

Public companies are also required to describe whether and how any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the company, including its business strategy, results of operations, or financial condition.^[181] Notably, the final rule requires disclosure of “processes” (as opposed to “policies and procedures”) in order to avoid requiring disclosure of operational details that could be exploited by threat actors

and make clear that companies without written policies and procedures need not disclose that fact. *Governance Disclosures*. The final rule also requires public companies to describe on Form 10-K how the board of directors oversees the company's cybersecurity risks. This includes identifying, if applicable, any board committee or subcommittee responsible for the oversight of cybersecurity risks and describing the processes by which the board or such committee is informed about such risks.^[182] Additionally, companies must describe management's role in assessing and managing the company's material cybersecurity risks from cybersecurity.^[183]

September 2023 – SEC Approves Revised Privacy Act Rule On September 20, 2023, the SEC approved a final rule, adopting amendments to the SEC's regulations under the Privacy Act of 1974, which governs the federal government's handling of personal information.^[184] The final rule updates and streamlines the SEC's Privacy Act regulations, including the process for submitting and receiving responses to Privacy Act requests and administrative appeals and provides electronic methods to verify an individual's identity.^[185] Given the extensive nature of the amendments, the final rule replaces entirely the current version of the Privacy Act regulations which was last updated in 2011. The final rule went into effect on October 26, 2023.

Cyber Rules for Registered Investment Advisers, Registered Investment Companies, and Business Development Companies Expected in April 2024. In February 2022, the SEC proposed cybersecurity rules for registered investment advisers, registered investment companies, and business development companies (the "RIA Rules").^[186] If adopted, the RIA Rules would require covered companies to, among other things, (i) adopt written cybersecurity policies and procedures to address cybersecurity risk, and (ii) report significant cybersecurity incidents, which are those that "significantly affect the critical operations" of a covered company or lead to "unauthorized access or use of information that results in substantial harm" to a covered company, or its clients, funds, or investors.^[187] As noted on the SEC's June 13, 2023 rulemaking agenda, the RIA Rules have entered the final rule stage^[188] and are expected to be finalized in April 2024.^[189] Looking ahead, the SEC Division of Examinations announced its priorities for 2024, which stated that it plans to continue focusing on "registrant's policies and procedures, internal controls, oversight of third-party vendors (where applicable), governance practices, and responses to cyber-related incidents."^[190] SEC Chair Gary Gensler emphasized that the "Division's efforts, as laid out in the 2024 priorities, enhance trust in our ever-evolving markets."^[191] Information security and cybersecurity will remain a key area of regulation and enforcement for the SEC in 2024.

b. Enforcement In addition to new rules, in 2023 the SEC continued to pursue enforcement actions at a historically high level against public companies, investment firms, law firms, and individuals.^[192] The SEC obtained orders totaling nearly \$5 billion in financial remedies in fiscal year 2023, the second-highest amount in SEC history following a record-setting nearly \$6.5 billion in fiscal year 2022.^[193] Notably, the SEC continued to focus on individuals, with about two-thirds of the SEC's cases in fiscal year 2023 involving individuals.^[194] The SEC also obtained orders that barred 133 individuals from serving as officers or directors for public companies, the highest such number in a decade.^[195] We expect these trends to continue in 2024, particularly as they relate to cybersecurity when the SEC's newly adopted cyber rules take effect and additional cyber rules are finalized. Below is a summary of some of the most notable cyber-related enforcement actions brought by the SEC in 2023.

Broker-Dealer Username/Password Handling Litigation. In September, 2023, the SEC alleged that a broker-dealer and its parent company allegedly made materially false and misleading statements and omissions regarding information barriers intended to prevent the misuse of sensitive customer information.^[196] The SEC alleged that the broker-dealer operated two businesses that were purportedly walled off from each other by data safeguards: a trade order execution service for institutional customers that typically operated on commission, and a proprietary trading business. However, during a 15-month period from 2018 to 2019, the broker-dealer allegedly failed to adequately safeguard a database of post-trade information regarding customer orders that included customer identifying information and further material nonpublic information.^[197] The broker-dealer allegedly rendered the database accessible to virtually anyone at its affiliates by leaving the data accessible via "two sets of widely known and frequently shared generic usernames and passwords."^[198] The SEC asserts that this alleged failure to safeguard the information posed significant risk that proprietary traders could abuse it or

distribute it outside the entity.^[199] The litigation remains pending. **Settlement for Allegedly Misleading Statements Related to 2020 Ransomware Attack.** In March 2023, the SEC imposed a \$3 million civil penalty to settle allegations it brought against a public company for making allegedly misleading disclosures concerning a 2020 ransomware attack that had impacted over 13,000 customers.^[200] The SEC alleged that, on July 16, 2020, the company announced a ransomware attacker had not gained access to customer bank account information or Social Security Numbers.^[201] Within days of the announcement, however, technology and customer relations personnel allegedly learned that the attacker had accessed and exfiltrated that sensitive information.^[202] The employees nonetheless allegedly failed to communicate this information to senior management accountable for its public disclosure because, in the SEC's view, the company failed to maintain adequate disclosure controls and procedures.^[203] As a result, the company's 10-Q report filed in August 2020 did not include this information about the cyberattack, which the SEC views as an omission of material information. In addition, the SEC alleged that the company's description of the risk of disclosure of sensitive customer information as a hypothetical risk was misleading.^[204] **SEC Alleges Fraud Against Public Company and its CISO.** In October 2023, the SEC alleged that a network monitoring software company and its Chief Information Security Officer ("CISO") engaged in fraud and internal controls violations.^[205] The SEC alleges that the company and its CISO overstated its cybersecurity practices and understated or failed to disclose known cybersecurity risks.^[206] The SEC's complaint alleges that the company's public statements conflicted with its internal assessments.^[207] The complaint also alleges that the CISO was aware of the company's cybersecurity risks, but failed to resolve the issues or sufficiently elevate them.^[208] The SEC alleged that the cybersecurity shortfalls rendered the company unable to provide reasonable assurances that its most valuable assets were sufficiently protected.^[209] The lapses in cybersecurity practices allegedly resulted in a two-year cyberattack campaign against the software company and some of its customers, including federal and state government agencies.^[210] The cyberattack was first disclosed publicly in December 2020, though the SEC alleged that disclosure was incomplete.^[211] According to the SEC, the company and CISO allegedly "paint[ed] a false picture of the company's cyber controls environment."^[212] The SEC alleged that the company and CISO violated antifraud provisions of the securities laws, that the company violated reporting and internal controls provisions, and that the CISO aided and abetted the company's violations.^[213] The SEC seeks permanent injunctive relief, disgorgement with prejudgment interest, civil penalties, and an officer-and-director bar against the CISO.^[214] Going forward, we expect to see a significant uptick in enforcement activity, particularly around cybersecurity disclosures, given the adoption of the SEC's cyber disclosure rules which went into effect in December 2023 and other proposed cyber rules pending finalization, as discussed above. **4. Department of Health and Human Services and HIPAA** On February 27, 2023, the Department of Health and Human Services ("HHS") announced three new divisions within the Office of Civil Rights ("OCR"): an Enforcement Division, a Policy Division, and a Strategic Planning Division.^[215] OCR enforces HIPAA and the Health Information Technology for Economic and Clinical Health Act of 2009, among additional privacy-related and other statutes.^[216] OCR explained that its caseload has increased 69 percent from 2017 and 2022.^[217] OCR thus created the new divisions to "improve[] OCR's ability to effectively respond to complaints, put[ting] OCR in line with its peers' structure and mov[ing] OCR into the future."^[218] The addition of three new divisions in OCR signals and underscores the heightened importance of data privacy and security within HHS. **a. Rulemaking on HIPAA Compliance and Data Breaches** On December 13, 2023, HHS finalized a rule implementing the 21st Century Cures Act that enhances the Office of the National Coordinator for Health Information Technology Certification Program, aimed at advancing interoperability, transparency, and the access, exchange, and use of electronic health information.^[219] The final rule is designed to increase algorithm transparency and information sharing for healthcare providers.^[220] The provisions of the rule are based on the principles of "fairness, appropriateness, validity, effectiveness and safety," and include certification criteria for "decision support interventions," "patient demographics and observations," "electronic case reporting," and the "exchange and use" of electronic health information.^[221] The final rule goes into effect on February 8, 2024.^[222] **b. Telehealth and Data Security**

Guidance HHS released a fact sheet in early 2023 identifying what will change as a result of the expiration of the federal Public Health Emergency for COVID-19 on May 11, 2023.^[223] HHS stated that the “vast majority” of current Medicare telehealth flexibilities (such as waivers of geographic and originating site restrictions and the allowance of audio-only telehealth services) will remain in place through December 2024.^[224] The agency also made some Medicare changes permanent so that they will stay in place now that the public health emergency has ended. These include allowing Federally Qualified Health Centers and Rural Health Centers to “serve as a distant site provider for behavioral/mental telehealth services,” allowing Medicare patients to “receive telehealth services for behavioral/mental health care in their home,” and allowing “behavioral/mental telehealth services” to “be delivered using audio-only communication platforms.”^[225] On July 20, 2023, the FTC and HHS issued a joint letter to 130 hospital systems and telehealth providers, warning them to “exercise extreme caution” with respect to certain online technologies that are incorporated in their websites and apps given the potential privacy risks these technologies may pose to patient data.^[226] The letter also reminded healthcare providers about their obligations under HIPAA and the FTC’s Health Breach Notification Rule.^[227] Relatedly, on September 15, 2023, the FTC and HHS issued an updated publication addressing businesses’ potential questions related to collecting, using, and sharing consumer health information, and provided links to more detailed guidance.^[228]

c. Reproductive and Sexual Health Data On June 24, 2023, HHS Secretary Xavier Becerra released a statement^[229] on the one-year anniversary of *Dobbs v. Jackson Women’s Health Org.*, which reversed *Roe v. Wade* and ended federal protection for abortion access.^[230] The statement highlights HHS’s efforts to protect and expand access to reproductive care, and outlines three “priority areas”:

1. “Reaffirming the Department’s commitment to protecting the right to abortion care in emergency settings under the Emergency Medical Treatment and Labor Act (EMTALA)”;
2. “Clarifying protections for birth control coverage under the Affordable Care Act”; and
3. “Protecting medical privacy – including empowering patients to protect their medical information on smart phones, apps, and other platforms.”^[231]

On April 12, 2023, HHS proposed measures to strengthen patient-provider confidentiality related to reproductive health care through a Notice of Proposed Rulemaking for the Privacy Rule.^[232] The proposed rule would prohibit the use or disclosure of protected health information (“PHI”) to identify, investigate, sue, or prosecute “patients, providers, and others involved in the provision of legal reproductive health care, including abortion.”^[233] The public comment period closed on June 16, 2023; and the proposed rule is expected to be finalized in March 2024.^[234]

d. HHS Enforcement Actions OCR continued to enforce the HIPAA Privacy Rule throughout 2023, which has been a continued focus of the agency in recent years. For example, OCR settled claims against a New York-based non-profit academic medical center for alleged violations in 2020 of the HIPAA Privacy Rule.^[235] A national newspaper published an article about the medical center’s COVID-19 emergency response, “which included photographs and information about the facility’s patients” exposing patient information, including COVID-19 diagnoses, medical statuses and prognoses, vital signs, and treatment plans.^[236] OCR alleged that the facility disclosed three patients’ protected health information to the press “without first obtaining written authorization from the patients.”^[237] The settlement required the facility to pay \$80,000 and agree to implement a corrective action plan “to develop written policies and procedures that [complied] with the HIPAA Privacy Rule.”^[238] HHS also focused its enforcement efforts around the HIPAA Right of Access Initiative, which was launched in 2019 and requires covered entities to provide individuals with “timely access to their health information for a reasonable cost” under the HIPAA Privacy Rule.^[239] As of December 15, 2023, OCR had brought 46 cases pursuant to the HIPAA Right of Access Initiative.^[240] These actions were largely brought against covered entities for failing to provide individuals with copies of protected health information within the required timeframe and/or in accordance with permitted fees.^[241] Data breaches have been

another recent priority. In February 2023, a nonprofit health system in Arizona agreed to pay \$1.25 million to resolve alleged HIPAA Security Rule violations arising from a 2016 data breach, which disclosed the protected health information of 2.81 million individuals.^[242] In addition to the monetary penalty, the hospital system agreed to implement a corrective action plan, and two years of OCR monitoring, to address alleged deficiencies relating to the protection of electronic PHI, including pertaining to risk assessment, vulnerability management, monitoring, authentication and protection of data transit.^[243] In December 2023, OCR also entered into a settlement with a Louisiana-based medical group for \$480,000, stemming from a phishing attack that exposed the personal information of over 34,000 individuals.^[244] OCR alleged that the group failed to conduct a risk analysis of potential vulnerabilities, as required under HIPAA.^[245] As with Banner Health, Lafourche agreed to implement a corrective action plan that OCR will monitor for two years.^[246]

5. Other Federal Agencies a. Department of Homeland Security In 2023, the Department of Homeland Security (“DHS”) continued to pursue various cybersecurity initiatives aimed at securing critical infrastructure and helping organizations respond to the rapidly evolving cyber threat landscape. The year marked an increased focus on cyber incident information sharing and reporting through public-private and cross-border partnerships. On March 2, 2023, DHS Secretary Alejandro N. Mayorkas released a statement about working to implement President Biden’s National Cybersecurity Strategy and emphasized the role of public-private sector collaboration and work with DHS’s Cyber Safety Review Board and Cybersecurity and Infrastructure Security Agency (“CISA”).^[247] As required by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (“CIRCA”), DHS and the Cyber Incident Reporting Council issued recommendations to Congress for streamlining the reporting of cyber incidents by establishing standard definitions, timelines, and triggers for reporting; creating a model incident reporting form for federal agencies; and creating a central reporting web portal.^[248] These recommendations will inform CISA’s ongoing rulemaking process, as it works towards publishing a Notice of Proposed Rulemaking related to CIRCA’s reporting requirements by March 2024.^[249] Secretary Mayorkas also hosted cyber leaders from 21 nations at the Western Hemisphere Cyber Conference to discuss bilateral and multilateral initiatives to respond to, and facilitate increased information sharing about, cybersecurity challenges, including around critical infrastructure and cyber-enabled crimes and ransomware.^[250] DHS also released multiple reports and advisories outlining recommendations to mitigate risks posed by threat actor groups and vulnerabilities affecting critical infrastructure, including malware attacks by the ransomware group CL0P against users of certain file-transfer software;^[251] targeting of industry-standard security tools by threat actor group Lapsus\$;^[252] and a ransomware variant used to exploit a vulnerability that threatened critical infrastructure.^[253] DHS also increased its State and Local Cybersecurity Grant Program funding from \$185 million in FY22 to \$374.9 million in FY23, signaling the growing importance of protecting communities from cyber threats.^[254]

b. Department of Justice In 2023, DOJ continued to focus on and expand its capacity to address cyber threats, especially those related to national security. In a series of press releases, DOJ touted certain accomplishments in its ongoing fight against organized cybercrime. For example, it publicized actions it had taken against several ransomware groups, including the Hive and Blackcat, as well as the malware code Qakbot. DOJ also announced significant developments regarding its approach to the issue of algorithmic bias, including an innovative resolution reached with a large social media company and the filing of a statement of interest in a case alleging racial discrimination against rental applicants. As part of its continued and expanding efforts to counter cyber-related national security threats arising from nation-state actors, DOJ created the National Security Cyber Section (“NatSec Cyber”) within the National Security Division (“NSD”).^[255] DOJ noted that NatSec Cyber “will allow NSD to increase the scale and speed of disruption campaigns and prosecutions of nation-state threat actors, state-sponsored cybercriminals, associated money launderers, and other cyber-enabled threats to national security.”^[256] DOJ continued its aggressive, multifaceted efforts to disrupt domestic and international organized cybercrime via collaboration between the FBI and foreign law enforcement organizations. For example, in January 2023, DOJ announced that its months-long campaign against a ransomware-as-a-service network called the “Hive” culminated in the seizure of thousands of decryption keys that were then distributed to victims of the Hive’s

activities, as well as the shutting down of servers and websites used by the Hive to coordinate attacks.^[257] The Hive’s ransomware campaign impacted more than 1,500 victims, “including hospitals, school districts, financial firms, and critical infrastructure,” across more than 80 countries, and sought to extort hundreds of millions of dollars in ransomware payments.^[258] In May 2023, DOJ publicized an operation code-named “MEDUSA,” which involved the deployment of an FBI-developed tool named “PERSEUS” to disrupt the ability of the highly sophisticated cyber espionage malware named “Snake” to compromise infected computers.^[259] Snake, whose development the U.S. government attributes to a unit in the Federal Security Service of the Russian Federation, has been used and adapted for the last nearly 20 years to steal and covertly transfer sensitive information from computer networks in over 50 countries, often in service of Russian interests.^[260] In August 2023, DOJ announced another multinational effort to degrade and avert attacks from Qakbot, a malware code used by cybercriminals to create malicious botnets and perpetrate “ransomware, financial fraud, and other cyber-enabled criminal activity.”^[261] Finally, in December 2023, DOJ announced that the FBI had successfully built a decryption tool that allowed victims of the ransomware-as-a-service group Blackcat (also known as ALPHV or Noberus) to regain control of their systems.^[262] This was in addition to taking control of websites associated with the group, which had previously carried out attacks targeting “government facilities, emergency services, defense industrial base companies, critical manufacturing, and healthcare and public health facilities—as well as other corporations, government entities, and schools,” costing victims hundreds of millions of dollars in ransom payments, incident response costs, and losses from data damage and theft.^[263] DOJ also waded into issues around algorithmic bias. In January 2023, for example, DOJ announced a resolution reached with a large social media company to address alleged algorithmic bias on its platforms.^[264] This development came as part of a settlement stemming from a June 2022 lawsuit filed in the U.S. District Court for the Southern District of New York that asserted the company engaged in discriminatory delivery of housing advertisements based on algorithms partially relying on protected characteristics in violation of the Fair Housing Act (“FHA”).^[265] The settlement agreement required the company to create a system (dubbed the Variance Reduction System) to promote the “equitable distribution of ads” across its platforms, subject to certain compliance metrics, oversight by the court, and ongoing monitoring by a third-party reviewer through June 27, 2026.^[266] A DOJ official praised the agreement and the company for setting “a new standard for addressing discrimination through machine learning” and called for others to follow the company’s lead. DOJ also filed a Statement of Interest in an FHA case pending in a Massachusetts federal district court brought by two Black rental applicants alleging unlawful algorithmic tenant screening practices.^[267] Plaintiffs alleged that the screening system discriminated “against Black and Hispanic rental applicants in violation of the FHA.”^[268] According to DOJ, the Statement confirms its “commitment to ensuring that the Fair Housing Act is appropriately applied in cases involving algorithms and tenant screening software.”^[269]

c. Department of Commerce

On March 7, 2023, a bipartisan group of senators proposed the Restricting the Emergence of Security Threats that Risk Information and Communications Technology (“RESTRICT”) Act, which would give the Commerce Secretary the power to ban foreign-owned technologies if they are found to pose national security threats.^[270] The bill, which received support from the Department of Commerce,^[271] was referred to the Committee on Commerce, Science, and Transportation, and is currently awaiting further action.^[272] On June 14, 2023, Senator Wyden introduced the Protecting Americans’ Data From Foreign Surveillance Act of 2023, which would update the Protecting Americans’ Data From Foreign Surveillance Act of 2022 that was introduced in June 2023 but not passed.^[273] This bill would bar exports of sensitive data to high-risk countries, as determined by the Department of Commerce.^[274] The Department of Commerce would also be tasked with defining sensitive data, though the bill broadly covers data, including browsing history and location data.^[275] However, the new export rules would not apply to data encrypted with technology approved by the National Institute of Standards and Technology (“NIST”).^[276] The bill was referred to the Committee on Banking, Housing, and Urban Affairs, and currently awaits further progress.^[277]

d. Department of Energy

Through the Infrastructure Investment and Jobs Act, the Department of Energy (“DOE”) has provided significant funding to a series of new cybersecurity programs.^[278] On

September 12, 2023, the DOE announced \$39 million of funding for nine new “National Laboratory” projects to strengthen the cybersecurity of distributed energy resources (“DER”).^[279] The funding is intended to “support targeted research, development, and demonstration related to different elements of the DER landscape.”^[280] Despite investing in improved cybersecurity for DER, the DOE itself continues to attract scrutiny of its cybersecurity practices, especially from the DOE’s Office of Inspector General (“OIG”). Ongoing concerns regarding the department’s cybersecurity capabilities stem in part from three apparent cyberattacks against DOE national laboratories in late 2022, which were serious enough to prompt House lawmakers to seek details concerning them in early 2023.^[281] In November 2023, the OIG released a report discussing “management challenges” at the DOE, including numerous cybersecurity-related deficiencies.^[282] In discussing these deficiencies, the report noted structural and resource-based challenges to an effective organization-wide cybersecurity program, some of which stemmed from inconsistent and outdated practices by DOE contractors.^[283] Thus, contractors/vendors doing business with the DOE should expect a greater emphasis on and scrutiny of their cybersecurity practices going forward.

e. Department of Defense In December 2023, the Department of Defense (“DoD”) released a proposal designed to implement its Cybersecurity Maturity Model Certification (“CMMC”) program, broadly aimed at increasing the security of controlled, unclassified information across the defense industry.^[284] The CMMC will set three “levels” of cybersecurity requirements based on the nature of information held by contractors, while ultimately creating a baseline level of cybersecurity for almost all DoD contract solicitations.^[285] The program will be implemented in phases over several years, giving companies time to study and understand its requirements and prepare staff to comply with them.^[286]

f. Federal Communications Commission The Federal Communications Commission (“FCC”) was particularly focused on the Telephone Consumer Protection Act (“TCPA”) and cybersecurity issues in 2023. In June 2023, the FCC unveiled a new Privacy and Data Protection Task Force that will “coordinate across the agency on the rulemaking, enforcement, and public awareness needs in the privacy and data protection sectors.”^[287] The task force will address issues such as data breaches of telecommunication providers linked to cyber intrusions and supply chain vulnerabilities.^[288]

TCPA Rulemaking. In January 2023, the FCC announced that new rules promulgated under Section 8 of the Telephone Robocall Abuse Criminal Enforcement and Deterrence (“TRACED”) Act^[289] would go into effect on July 20, 2023.^[290] Among other things, the FCC’s new rules provide additional clarity on exemptions from the TCPA, including establishing limits on the number of exempt calls that can be made to a residence during a 30-day period (for non-commercial, non-advertising, or nonprofit purposes); requiring callers to obtain consent before exceeding the numerical limits on exempt calls; and mandating ways that consumers can opt out of exempted calls to residential lines.^[291] In the last quarter of 2023, the FCC took additional regulatory steps to curb robocalls. On October 23, 2023, FCC Chairwoman Jessica Rosenworcel announced the FCC was opening an inquiry into the impact of artificial intelligence technology on robocalls, particularly for more vulnerable consumers such as seniors and those on fixed incomes.^[292] Following that announcement, the FCC sought public input to better understand the impact of emerging AI technologies on unwanted telephone calls and text messages.^[293] It seems likely that the FCC will continue to assess AI’s impact in this area. On December 18, 2023, the FCC also approved new TCPA rules that require lead generators, comparison shopping websites, and similar companies to obtain a consumer’s prior express written consent to receive automated calls from each marketing partner.^[294] The rule is intended to end companies’ prior practice of relying on a single consent to receive automated calls from multiple marketing partners. The new rule has closed this loophole, and requires one-to-one consent for each marketing partner.^[295] There will be an implementation period of at least 12 months to allow companies to make necessary changes to ensure consent complies with the new rules.^[296]

Cyber Trust Mark. In July 2023, the FCC, in coordination with the White House, announced a proposal to create a “U.S. Cyber Trust Mark” label for devices that meet certain cybersecurity and privacy criteria set by the National Institute of Standards and Technology, with voluntary commitments to the standard to be made by manufacturers and retailers.^[297] Examples of contemplated features offered by labeled

devices include “unique and strong default passwords, data protection, software updates, and incident detection capabilities.”[\[298\]](#) In August 2023, the FCC released a Notice of Proposed Rulemaking regarding the proposal to collect public input, noting that if it votes to establish the program, it could be “up and running” by late 2024.[\[299\]](#) **VoIP and TRS Rules.** In December 2023, the FCC approved modifications to data breach notification rules for providers of telecommunications, interconnected Voice over Internet Protocol (“VoIP”), and telecommunications relay services (“TRS”).[\[300\]](#) The modifications expand reportable personally identifiable information and the definition of a “breach,” and require carriers or TRS providers to notify the FCC of breaches, in addition to other existing reporting requirements.[\[301\]](#) **Enforcement.** The FCC also levied fines against companies for lax data security standards. In July 2023, the FCC sought a combined \$20 million fine against two mobile carriers for alleged violations of FCC rules, which mandate that customer identity be properly authenticated before online access to Customer Proprietary Network Information (“CPNI”) is granted to them.[\[302\]](#) The FCC’s investigation concluded that the companies used “readily available” information to provide online access to CPNI and fell below other compulsory data security standards in violation of multiple parts of the FCC’s rules, thereby placing sensitive customer personal data at risk.[\[303\]](#)

6. State Agencies Throughout 2023, state privacy enforcers, particularly in California, wielded their authority to attempt to expand the ambit of existing privacy laws. **a. California** California Privacy Protection Agency On the rulemaking front, the California Privacy Protection Agency (“CPPA”) released draft rules for automated decision-making technology (“ADMT”) on November 27, 2023.[\[304\]](#) The draft focuses on two areas: notice requirements on the use of ADMT and enforcement of two new consumer rights: the right to opt-out of ADMT processing and the right to access information about a business’s use of ADMT. The draft rules require businesses to provide a “Pre-use Notice” which would allow consumers to exercise these two rights. The notice must inform consumers of the business’s use of ADMT and permit them to opt-out of ADMT processing. It also requires businesses to describe the purpose behind the use of ADMT in specific terms. Consumers may opt-out of ADMT for decisions that produce “legal or similarly significant effects” (1) as an employee, student, job applicant or independent contractor or (2) in publicly accessible places (e.g., via surveillance or facial recognition). Formal rulemaking is expected to begin in early 2024. The CPPA has also begun to spin up its enforcement division, which began inquiring into manufacturers of connected vehicles, meaning vehicles embedded with features like location sharing, web-based entertainment, smartphone integration, and cameras, in an effort to better understand whether companies in this space are complying with applicable rules.[\[305\]](#)

California Attorney General The California Attorney General (“CA AG”) has announced several privacy-related enforcement “sweeps” in 2023 in a variety of industries. In early 2023, the CA AG sent out letters to an unspecified number of mobile apps in the retail, travel, and food service industries that purportedly failed to comply with the CCPA, specifically by failing to honor consumer requests to opt out of the sale of their personal data or providing mechanisms for opting out of sale of the personal data.[\[306\]](#) In July 2023, the CA AG announced a separate sweep of large employers’ compliance with CCPA as it related to employee and job applicant information.[\[307\]](#) Businesses are required to provide a way for consumers, workers, and job applicants to be able to access, delete, and opt-out of the sale of their personal information. Despite these regular sweeps, however, the CA AG has not announced any enforcement actions or settlements related to the CCPA. Although there have not been any CCPA settlements disclosed in 2023, the CA AG did announce a \$93 million settlement with a large technology company related to allegations that its location-privacy practices violated California’s Unfair Competition Law, a follow-on to a multistate settlement announced in 2022.[\[308\]](#) The complaint alleged that the company deceived people into consenting to the perpetual collection and use of their location data by asking users if they wanted to “enhance” their “experience.” The complaint also alleged that, even if users turned off their location history, their precise location data was nevertheless collected if other settings remained enabled. Finally, the CA AG alleged that the company continued to use real-time location information to show users ads, even if they turned off ad personalization. Under the terms of the settlement, the company will have to provide a pop-up notification to users who have certain location-tracking toggles enabled, provide additional disclosures to users (including in the account-creation flow) and obtain express

affirmative consent prior to sharing precise location information with advertisers, among other requirements. The company will also have to submit an annual compliance report and independent assessor reports. **b. Other State Agencies** New York In January 2023, the New York Attorney General (“NY AG”) sent a letter to a large live-entertainment company about its use of facial recognition technology that allegedly was preventing entry into its venue by attorneys whose firms are engaged in litigation against the company.^[309] The NY AG’s letter requests the company provide justifications for its policy, identify efforts to comply with applicable laws, and ensure that its use of this technology will not lead to discrimination. In November 2023, the New York State Department of Financial Services announced that a title insurer will pay \$1 million for allegedly violating state cybersecurity regulations.^[310] The insurer allegedly failed to ensure “full and complete implementation” of its cybersecurity policies and procedures prior to a May 2019 data breach that exposed its customers’ nonpublic information.^[311] Washington The Washington Attorney General (“WA AG”) announced a \$39.9 million settlement with a large technology company related to the WA AG’s lawsuit over its location-tracking practices.^[312] The WA AG, like the CA AG, filed a separate lawsuit from the multistate effort that had been settled in November 2022. Similar to the California suit, the WA AG alleged that the company collects location data even when consumers had disabled their location history and that it tracked devices even when location access was turned off. In addition to the monetary penalty, the company agreed to disclose additional information to users where they enabled location-related account setting, ensured that users see information about location tracking and gave users detailed information about types of location data that the company collects and how it will be used. **c. Major Data Breach Settlements** While 2023 did not see as many high-profile data breach settlements as in recent years, with the number of data breach-related case filings reaching new records, major settlements are likely on the horizon. Many of the notable 2023 settlements were reached with state attorneys general. A software provider in the healthcare and education space agreed to a \$49.5 million settlement with numerous state attorneys general (led by Indiana and Vermont) to resolve claims stemming from a ransomware attack that impacted the company and nearly 13,000 customers in 2020.^[313] In another notable data breach settlement, the attorneys general of New York, Connecticut, Florida, Indiana, New Jersey, and Vermont entered into a \$6.5 million settlement with a major financial services provider arising from two instances in which customer data inadvertently left the company’s custody.^[314] And a vision insurance company entered a \$2.5 million settlement with the attorneys general of New Jersey, Oregon, Florida, and Pennsylvania stemming from a breach which impacted the health care information of 2.1 million individuals.^[315] Class actions have also resulted in significant settlements. A law firm recently announced that it reached a tentative class settlement with plaintiffs whose personal information was allegedly compromised in a data breach.^[316] Once finalized, this settlement will resolve four consolidated lawsuits stemming from the firm’s alleged three-month delay in notifying affected individuals of the breach. And in July 2023, the Southern District of Florida approved a \$3 million settlement in a class action suit against a health care network and its parent company arising from a 2021 data breach in which over three million individuals were affected.^[317] **III. Civil Litigation Regarding Privacy and Data Security** **A. Data Breach Litigation** Cybercrimes targeting consumer data have been increasingly pervasive and this trend continued in 2023. The Identity Theft Resource Center, which compiles statistical information on data breaches, reported 2,116 data breaches in the first nine months of 2023.^[318] This number surpasses the 2021 record of 1,862 data breaches and represents a nearly 64% increase of the number of data breaches reported over the same nine-month period in 2022.^[319] These trends suggest companies will continue to face more widespread and sophisticated attacks by cybercriminals and the risk of litigation remains elevated for companies dealing with the aftermath of a cyberattack. One of the largest and most significant data breach litigations in history was filed this year. After the developer of a popular file transfer service announced that its service had been exploited by a Russian cybergang in a data breach that exposed the personally identifiable information of more than 55 million people, more than 200 cases were filed.^[320] These actions were centralized in an MDL that is now pending in the District of Massachusetts.^[321] At the time of publication, the MDL remains in its early stages, but we expect this case will be one that practitioners will watch closely.

This section summarizes key developments in data breach litigation last year. **1. The Impact of *TransUnion v. Ramirez* on Standing in Data Breach Actions** Many data breach cases are litigated in federal court, given large numbers of potentially affected individuals and jurisdictional provisions of the Class Action Fairness Act. Plaintiffs pursuing claims in federal court must satisfy the standing requirements of Article III of the U.S. Constitution, and data breach actions raise significant questions about whether plaintiffs can satisfy this requirement. In 2021, the U.S. Supreme Court decided *TransUnion v. Ramirez*, a landmark decision that increased the burden on plaintiffs to demonstrate standing in actions for money damages brought in federal court.^[322] The Court held that the mere risk of future harm is insufficient to satisfy the concrete injury that Article III requires, especially where the plaintiff is unaware of the risk of future harm.^[323] This holding is especially significant in data breach cases where a plaintiff's data has been breached but not yet misused. Although *TransUnion* went a long way towards clarifying how risks of future harm should be analyzed under Article III, appellate courts have continued to grapple with the bounds of the Court's holding and divergent approaches to the issue of standing persisted in 2023. Some courts have interpreted *TransUnion* narrowly and concluded that notwithstanding its holding, plaintiffs can establish standing even if their data has not yet been misused. For example, in *Webb v. Injured Workers Pharmacy, LLC*, the First Circuit held that a "material risk of future harm can satisfy the concrete-harm requirement" for standing, reasoning that data compromised in targeted attacks (as opposed to inadvertent disclosures) is more likely to be misused, especially when the data is sensitive and other personal information in the exposed data has already been misused.^[324] Moreover, to satisfy *TransUnion's* requirement of "alleg[ing] a separate, concrete present harm" to have standing to seek damages, the court held that the plaintiffs' "time spent responding to a data breach can constitute a concrete injury sufficient to confer standing, at least when that time would otherwise have been put to profitable use."^[325] Similarly, the Second Circuit held that a plaintiff suffered "concrete harms as a result of the risk of future harm occasioned by the exposure" of her personal information, in particular because she incurred expenses attempting to mitigate the consequences of the breach.^[326] Moreover, the plaintiff's name and Social Security number were compromised in the targeted attack, and the court reasoned that the exposure of this type of sensitive data led to concrete present harms due to the increased risk that her identity would be stolen in the future.^[327] Other courts have interpreted *TransUnion* to mandate a stricter approach to standing. For example, in *Holmes v. Elephant Insurance Co.*, a trial court dismissed for lack of standing claims alleging that the plaintiffs' personal information was compromised in a 2022 data breach.^[328] Despite a potential heightened risk of future identity theft, the court found that this risk alone did not constitute an injury in fact unless it was "certainly impending."^[329] Even though two of the three named plaintiffs had alleged their driver's license information had appeared on the dark web, the court reasoned that unless combined with additional personal information, a driver's license number could not be used to create a full identity profile, and therefore only constituted a threat of future identity theft.^[330] The court also found there was insufficient support for the contention that the risk of identity theft was "certainly impending" without assuming that the plaintiffs were specifically targeted in the breach, that the perpetrator was actively compiling full profiles of plaintiffs, and that the perpetrator would "imminently and successfully attempt to use th[e] information [at issue] to steal the plaintiffs' identities."^[331] In reaching this conclusion, the court also diverged from the approach taken by the First Circuit in *Webb*, finding that absent an imminent threat of identity theft, the cost of mitigative measures, such as time spent monitoring financial information, does not constitute an injury sufficient to support standing.^[332] A California district court in *Burns v. Mammoth Media, Inc.*, appeared to agree with this approach, suggesting that "an increased risk of identity theft may constitute a credible threat of real and immediate harm sufficient to constitute an injury in fact for standing purposes."^[333] However, the court ultimately denied standing and dismissed the claims because there were insufficient allegations to establish an increased threat of identity theft based on the type of data compromised. In particular, the plaintiff alleged only that his name, email address, gender, profile creation date, user name, user ID, password, and access token were exposed, but he failed to explain how the specific data compromised was sufficiently sensitive to create a risk of identity

theft.^[334] Questions about standing are also significant to class certification, as putative classes that contain large numbers of uninjured class members are frequently not viable.^[335] One case from 2023 illustrating this issue is *Attias v. CareFirst, Inc.*, where the District Court for the District of Columbia denied class certification because “the proposed classes . . . would appear to sweep in significant numbers of people who have suffered no injury in fact in light of *TransUnion*.”^[336] Even though the named plaintiffs had adequately demonstrated standing “because they ha[d] spent at least some amount of time or money protecting against the risk of future identity theft,” there was a “serious predominance problem” because not all the putative class members had done the same, thereby necessitating “individualized proof of injury.”^[337] These “logistical hurdles of identifying class members who were injured or determining what kinds of mitigation measures might qualify an individual for class membership” meant the court “[could not] conclude that the common issues predominate over individualized inquiries.”^[338]

2. Cybersecurity-Related Securities Litigation

In the aftermath of a cybersecurity incident, companies and their officers also frequently face shareholders suits. Although the pace of data breach-related securities case filings has slowed,^[339] the past year still saw a fair share of new litigation. For instance, in March 2023, shareholders filed a securities class action under Sections 10(b) and 20(a) of the Securities Exchange Act of 1934 against a television service provider, alleging that the company overstated its operational efficiency in public statements and SEC filings and maintained deficient cybersecurity infrastructure, leaving the company unable to secure customer data and leaving it vulnerable to cyberattacks and service issues.^[340] In another action filed in 2023, shareholders alleged that a financial services technology company violated Sections 12(a)(2) and 15 of the Securities Act of 1933 in connection with the compromise of customer data.^[341] The plaintiffs alleged that the company failed to accurately describe its data security capabilities, among other things, in its securities filings. This case remains in the early stages. Defendants have had success in getting shareholder data-breach claims dismissed on the pleadings, including for failure to plead falsity or scienter with the requisite particularity.^[342] For example, the Northern District of California dismissed a shareholder suit related to a January 2022 data security incident.^[343] The plaintiffs in that case sued under Section 10(b) and 20(a) of the Securities Exchange Act of 1934, alleging that the company and certain officers made false and misleading statements in the company’s disclosures about its data security practices.^[344] The court dismissed these allegations, finding that the plaintiffs failed to allege either falsity or scienter based on the defendants’ general statements about the company’s commitment to data security.^[345]

B. Wiretapping and Related Litigation Concerning Online “Tracking” Technologies

[Last year’s Review](#) noted a deluge of lawsuits brought under federal and state wiretapping statutes. This trend continued in 2023, with recent lawsuits alleging that various businesses invade consumers’ privacy rights and violate federal and state wiretapping statutes by allegedly failing to obtain sufficient and valid consent when using various online “tracking” technologies, such as session replay, pixels, and chat software. Plaintiffs in these cases generally allege that their interactions with businesses’ websites or apps are “communications” between them and the business, which are being “recorded” and “intercepted” by the business through a third-party pixel, software development kit, chat, or session-replay service provider.^[346] Many of these cases focus on claims for violations of wiretapping statutes. Wiretapping statutes were initially intended to prevent surreptitious recording of, or eavesdropping on, phone calls without the consent of the parties involved, but they have evolved to cover other forms of electronic and digital communications. The federal Wiretap Act of 1968, as amended by the Electronic Communications Privacy Act of 1986,^[347] is a “one-party” consent statute that allows communications to be intercepted (with certain exceptions) so long as “one of the parties to the communication has given prior consent[.]”^[348] Almost all 50 states also have some form of wiretapping statute; most of them are also one-party consent statutes, but a significant minority require “two-party” (or “all-party”) consent.^[349] Many recent lawsuits have brought claims under both the federal Wiretap Act and various state statutes, with litigation heavy in all-party consent states like California (where statutory damages can run as high as \$5,000 per violation), Pennsylvania, and Florida.^[350] In addition to alleged violations of wiretapping statutes, lawsuits concerning online tracking technologies frequently raise a host of interrelated legal issues. For example, a plaintiff in a Northern District of California case alleged that a

pixel tool was embedded in a university-owned hospital website where the plaintiff entered private medical information concerning her cardiovascular health.^[351] Because this information was allegedly redirected to a third-party company, the plaintiff claimed that the defendant violated the California Invasion of Privacy Act (“CIPA”), three separate sections of the Confidentiality of Medical Information Act (“CMIA”), and the California Constitution. The plaintiff also alleged common law causes of action including breach of contract, unjust enrichment, and the right to privacy. The court allowed the common law privacy and two CMIA claims to move forward and dismissed the remaining claims, largely on the basis that the university is an immune public entity. Similarly, in *Jackson v. Fandom Inc.*,^[352] another Northern District of California judge denied the defendant’s motion to dismiss a proposed class action alleging that the defendant, a hosting service for user-generated wikis, violated the federal Video Privacy Protection Act (“VPPA”) by sharing users’ personally identifiable information (“PII”) through pixels. Specifically, the judge found that associating viewing history with the plaintiff’s unique user ID may have constituted unlawful disclosure of PII.^[353] In yet another notable decision, a federal judge dismissed claims against a technology company alleging it had shared information about the plaintiffs’ online activity with a third party via a pixel without the plaintiffs’ consent.^[354] The plaintiffs claimed that the company’s terms of use did not inform users that the platform was sharing information with the third party and that its failure to disclose this information was fraud by omission in violation of both California’s Unfair Competition Law (“UCL”) and its Consumer Legal Remedies Act (“CLRA”). They also asserted claims under VPPA and for unjust enrichment. In granting the company’s motion to dismiss these claims, the court reasoned that Rule 9(b)’s heightened pleading standard applied because the alleged fraud stemmed from alleged misrepresentations in the company’s terms of use.^[355] The court therefore granted the company’s motion to dismiss the CLRA and UCL claims. In November 2023, the company moved for summary judgment on that claim, which remains pending. These cases are representative of many others, and we expect plaintiffs to leverage their mixed outcomes to continue to bring and attempt to extract settlements in similar matters.

C. Anti-Hacking and Computer Intrusion Statutes The federal Computer Fraud and Abuse Act (“CFAA”) generally makes it unlawful to “intentionally access a computer without authorization” or to “exceed[] authorized access.”^[356] In recent years, several high-profile court decisions, including the U.S. Supreme Court’s 2021 decision in *Van Buren v. United States*, have limited the CFAA’s scope.^[357] In 2022, these decisions also prompted the Department of Justice to narrow its CFAA enforcement policies,^[358] as described in [last year’s Review](#).

1. CFAA In 2023, courts around the country have continued to grapple with the CFAA’s outer bounds. Summarized below are three cases of particular interest, including a case from the Second Circuit analyzing venue considerations in CFAA actions and a pair of district court cases reaching somewhat different conclusions on whether software constitutes a “computer” under the statute.

Venue in CFAA Criminal Cases. In July 2023, the Second Circuit upheld a criminal CFAA conviction against a venue challenge.^[359] The case involved a defendant, a disgruntled former employee, who deleted information from her company’s online database, which was hosted on servers outside of New York.^[360] Her deletion of the database prevented some employees in New York from accessing it.^[361] A criminal action was brought against the defendant in the Southern District of New York and the defendant argued venue was improper because the data she deleted resided on servers in Virginia and California, and therefore she could not have damaged a computer in New York.^[362] The Second Circuit rejected this claim, holding that even though the data was stored on cloud servers elsewhere, the defendant had still “damaged” a computer in New York, because she had “impair[ed] . . . the integrity or availability of data, a program, a system, or information” on a computer there.^[363] The Supreme Court denied certiorari.^[364] The case is notable not just because of its expansive view of venue in CFAA criminal cases, but also because it raises new questions about the scope of covered harm to “protected computers” in CFAA criminal and civil cases alike—an especially important issue given the interconnectedness of computer networks.

Cloud Computing Systems As Covered “Computers.” In July 2023, an Illinois federal district court held that a “cloud-based system of data storage” constitutes a “computer” under the civil enforcement sections of the CFAA.^[365] The defendants in this case allegedly accessed a former employer’s Microsoft Office 365 cloud services after their employer

terminated them—by logging in with old and phony credentials.^[366] The defendants moved to dismiss the employer’s CFAA claim, arguing a cloud service is not a protected “computer” under the CFAA.^[367] The court disagreed.^[368] The court reasoned that the CFAA broadly defines a “computer” as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”^[369] Because a cloud system involves storing data on remote servers, and “[s]ervers fit within the plain language” of a computer under the Act, the plaintiff had sufficiently alleged that the defendants improperly accessed a “computer” under the CFAA.^[370] The court also rejected the premise that CFAA liability could attach only if the *plaintiff*, rather than Microsoft, actually owned the remote servers that supported the cloud service.^[371] **Software Not a Covered “Computer.”** By contrast, in April 2023, a New Jersey federal district court held that “software” does not constitute a protected computer under the CFAA.^[372] In this case, the plaintiff claimed that he was hired to install certain software he created on a bank’s computers, but a dispute arose over whether the bank had paid for a license to use the software.^[373] The plaintiff sued, claiming, among other things, that by using the software without permission and by locking him out of his bank computer (which allegedly contained the software), the bank violated the CFAA.^[374] The court summarily disagreed, noting that the plaintiff had presented “no authority indicating that software is a ‘computer’ within the meaning of the CFAA,” and dismissed the claim.^[375] **Generative AI and the CFAA.** Another notable development from this past year was the bevy of lawsuits filed against generative AI companies, challenging the companies’ alleged practice of scraping or otherwise obtaining data to train their AI models. Some of these lawsuits claim that these practices—which involve allegedly harvesting publicly accessible data from the Internet or obtaining user data through the use of “plug-ins” installed on third-party websites—violate the CFAA for exceeding authorized access to plaintiffs’ computers.^[376] These cases are still at their early stages and will likely need to grapple with the Ninth Circuit’s 2022 decision in *hiQ Labs, Inc. v. LinkedIn*.^[377] which held that the CFAA’s concept of “without authorization” may not apply “when a computer network generally permits public access to its data”—although the Ninth Circuit noted there may be other common law and statutory claims available for those who believe they have been the victims of data scraping.^[378] **2. CDAFA** The Comprehensive Data Access and Fraud Act (“CDAFA”) is California’s sister statute to the CFAA, and it creates a private right of action against any person who “[k]nowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.”^[379] “Access” means to “cause output from” the “logical, arithmetical, or memory function resources of a computer.”^[380] In 2023, several district courts considered the interaction between the CDAFA and the recent wave of litigation related to website tracking technologies, including web pixels. Below are two such cases of interest. **Private Browsing Modes and Online Advertising Technologies.** In August 2023, a California district court denied a motion for summary judgment on a CDAFA claim. Plaintiffs alleged that a prominent internet company improperly tracked user activity when users were using “private browsing modes.”^[381] Plaintiffs claimed that, when third parties embedded certain advertising technologies into their websites, those technologies sent data about the users’ online activities to the company, even if the users were using a private browsing mode.^[382] The company sought summary judgment on plaintiffs’ CDAFA claim, arguing that the company could not have “accessed” plaintiffs’ computers under the CDAFA because “website developers,” not the defendant, embed the code that directs users’ browsers to send requests to the company’s servers.”^[383] The court rejected this argument, holding that the fact that “website developers chose to embed [the company’s] services onto their websites at most creates a triable issue as to whether developers and not the company . . . ‘cause output from’ plaintiffs’ computers” under the CDAFA.^[384] The company separately argued that plaintiffs had suffered no “damage or loss” under the CDAFA, but the court rejected this argument, too, holding that “plaintiffs [had] proffer[ed] evidence that there is a market” for their browsing history data.^[385] On December 26, 2023, the parties announced that they had reached a preliminary settlement agreement.^[386] **“Technical Barriers” for First-Party**

Websites. In October 2023, a California district court dismissed with prejudice a CDAFA claim premised on the theory that a chatbox on a developer's website transmitted certain user information to third parties.^[387] The developer argued that it did not act "without permission" under the CDAFA because it did not overcome any "technical or code-based barriers" to insert the third-party code into its own website and allegedly transmit user information.^[388] The district court agreed, holding that there are "no technical barriers blocking Defendant from using its own Website" in the manner alleged.^[389] The district court also dismissed the claim on the basis that plaintiff had failed to allege any damage or loss under the CDAFA.^[390]

D. Telephone Consumer Protection Act Litigation Originally enacted in 1991, the Telephone Consumer Protection Act ("TCPA") regulates certain forms of telemarketing and the use of automatic telephone dialing systems ("ATDS").^[391] Historically, much of TCPA litigation centered on issues concerning the technical definition of an ATDS, but that issue was largely clarified through the Supreme Court's 2021 opinion in *Facebook Inc. v. Duguid*, which favored a narrower definition that limited it to devices that store or produce telephone numbers by using a random or sequential number generator.^[392] Nonetheless, the TCPA continues to be an area of significant regulatory and litigation activity. 2023 was defined by increased regulation and enforcement by the FCC, as well as ongoing federal litigation addressing the scope of the TCPA. TCPA cases continue to make their way up to the federal appellate courts, which frequently present the issue of whether receipt of a single unsolicited call is sufficient to confer Article III standing. Some circuits have answered in the affirmative. For example, the Sixth Circuit held that a consumer who had received a ringless voicemail had standing to sue under the TCPA.^[393] The plaintiff argued, successfully, that the receipt of the unsolicited ringless voicemail was comparable to the common law tort of intrusion upon seclusion.^[394] Similarly, in *Drazen v. Pinto*, an en banc panel of the Eleventh Circuit held that individuals who received even a single unwanted telemarketing text message had standing to sue under the TCPA, overruling the court's prior decision that held the opposite.^[395] In another notable decision, *Hall v. Smosh Dot Com, Inc.*, the Ninth Circuit held that a phone line subscriber has standing to sue for TCPA violations, even if the subscriber is not the recipient of the call.^[396] Even though the plaintiff's son in that case had received the unwanted text messages, the Ninth Circuit stated that the TCPA does not require that "the owner of a cell phone must also be the phone's primary or customary user to be injured by unsolicited phone calls or text messages sent to its number."^[397] Not all courts have read the TCPA so expansively, and appellate courts continue to find communications not covered by the language of the TCPA. For example, in January 2023, the Third Circuit held that faxes sent by a drug testing laboratory, promoting a free educational seminar about opioid use and medication monitoring, did not qualify as "unsolicited advertisements" under the TCPA.^[398] In another notable case, the Ninth Circuit held that text messages did not violate the TCPA's prohibition on "prerecorded voices," because text messages are not "voice" messages.^[399] In the face of newly implemented rules, shifting case law, and new communications technology, we expect the TCPA to continue to be an area to watch.

E. State Law Litigation 1. California Consumer Privacy Act Litigation While the regulatory atmosphere around the CCPA evolved in 2023, the litigation landscape remained fairly constant. Consumers, individually or as a class, continued to litigate under the CCPA, making claims for both pecuniary and statutory damages.

a. Potential Anchoring Effect of CCPA Statutory Damages As discussed in [last year's Review](#), the CCPA's provisions for statutory damages have continued to frame settlement negotiations. The CCPA provides that consumers exercising their private right of action for a data breach may recover the greater of statutory damages between \$100 and \$750 per consumer, per incident, or actual damages.^[400] The cases summarized below provide color on how these statutory damages have impacted settlement terms in the CCPA context.

Automobile Manufacturers and Marketing Vendor. In this case, previously discussed in [last year's Review](#), residents of California and Florida filed class actions alleging that auto manufacturers and a marketing vendor failed to adequately secure customers' personal information, allowing hackers to steal information such as driver's license numbers, Social Security numbers, financial account numbers and more.^[401] The plaintiffs asserted causes of action for negligence, breach of implied contract, violation of the CCPA, violation of California's Unfair Competition Law, and breach of contract. The parties agreed to a

settlement which was granted final approval on May 31, 2023.^[402] The terms of the settlement reflect the potential effects of the CCPA, as California residents whose sensitive personal information was affected received \$350, while the non-California residents whose sensitive personal information was exposed would receive only \$80 (about 77% less than their California peers).^[403] **Ticket Retailer.** Consumers who bought tickets from a ticket retailer brought suit after a data breach was disclosed. Plaintiffs alleged that “skimmers” placed on the defendant’s checkout webpage stole their personal sensitive data.^[404] Plaintiffs asserted a variety of claims, including negligence, breach of contract, violation of California’s Unfair Competition Law, and violation of the CCPA.^[405] The parties reached a \$3 million settlement, which was granted final approval on October 30, 2023. The settlement fund provides California sub-class members with an additional \$100 “California Statutory Award benefit.”^[406] **b. Requirements for Adequately Stating a CCPA Claim** Courts continued to give shape to the requirements to plead a CCPA claim. The decisions below address the facts and allegations required to bring a CCPA action under its limited private right of action, which applies only to data breaches.

Software Company Automatic Renewal Case. The Ninth Circuit recently affirmed the dismissal of a case alleging violations of the CCPA. The plaintiff alleged his data was shared with a credit card processor without his authorization due to the automatic renewal of his subscription. The trial court dismissed his claim because the plaintiff had agreed to the defendant’s End-User License Agreement, which stated his subscription would renew every 12 months unless terminated.^[407] The trial court found the disclosure of his personal information was not “without authorization” and was not caused by a failure to implement reasonable security procedures and practices.^[408] The Ninth Circuit affirmed.^[409] **Online Banking.** Plaintiff alleged that the defendant bank violated the CCPA when an unknown individual accessed his bank account, changed his contact information, and obtained new account cards to make purchases. The bank, on a motion to dismiss, argued that the plaintiff had not alleged that a data breach occurred. The court disagreed, finding that plaintiff’s allegations that his account was accessed and personal information obtained because of the failure to implement reasonable security procedures were sufficient to state a claim under the CCPA.^[410] **c. CCPA Violations Under the UCL** Violations of the CCPA cannot serve as the predicate for a cause of action under a separate statute including California’s Unfair Competition Law (“UCL”).^[411] While there has been no change regarding the inability to use a CCPA violation as the predicate “unlawful” claim under the UCL, one court has found the CCPA may create a property interest upon which a UCL claim may be brought. That decision is summarized below.

Search Engine Company. Originally filed in June 2020, this class action alleges that a large technology company unlawfully collected data from users while using the company’s browser in incognito or private mode.^[412] The plaintiffs brought claims, including under the federal Wiretap Act, the California Invasion of Privacy Act (CIPA), and California’s UCL.^[413] On summary judgment, the defendant argued that plaintiffs had no economic injury as required for a UCL claim, as they had not lost money or property as a result of the data collection.^[414] Plaintiffs argued that their private data has monetary value and they have a property interest in that data “because the [CCPA] affords them the right to exclude Google from selling their data to third parties.”^[415] The court agreed with plaintiffs, holding that “plaintiffs have identified an unopposed property interest for at least a portion of the class period under the California Consumer Privacy Act.”^[416] The court further found that money damages are not an adequate remedy alone, and that injunctive relief is necessary to address the ongoing data collection.^[417] **d. The CCPA’s 30-Day Notice Requirement** The CCPA requires that a “consumer provide[] a business 30 days’ written notice identifying the specific provisions of [the CCPA] the consumer alleges have been or are being violated.”^[418] The written notice initiates a 30-day period during which the business may cure any violation. While this cure provision was eliminated by the CPRA, cases addressing the notice-and-cure provisions have continued to move through the courts. [Last year’s Review](#) discussed a case dismissing a suit with prejudice where plaintiffs did not comply with the 30-day notice period.^[419] The cases below have departed from that decision, illustrating the boundaries of the cure provision as a safeguard. **Consumer Debt Collector.** Plaintiffs alleged that their personal information was stolen in a data breach because the information was unencrypted and improperly safeguarded.^[420] Plaintiffs brought claims under the CCPA for actual and statutory

damages, even though they provided no pre-suit notice for the defendant to cure as required under the CCPA.^[421] The court noted that no pre-suit notice is required to the extent plaintiffs sought pecuniary damages, but dismissed the statutory damages claims without prejudice.^[422] In dismissing the claim for statutory damages without prejudice, the court expressly declined to follow *Griffey*, which we discussed in [last year's Review](#). The *Griffey* court had dismissed a CCPA claim with prejudice, reasoning that the purpose of the pre-suit notice is to allow the defendant time to cure the violation out of court.^[423] Allowing a plaintiff to file a complaint, then send a notice, and then file an amended complaint defeats this remedial purpose of the statutory notice-and-cure provision. The Western District of Washington expressly rejected *Griffey's* rationale, concluding that dismissal without prejudice “accords with the remedial nature of the CCPA’s notice provision.”^[424] **Money Services Business.** After a data breach, plaintiffs brought suit claiming negligence, breach of implied contract, and violation of the CCPA due to the disclosure of their names, Social Security numbers, and driver’s license numbers.^[425] Defendant moved to dismiss the CCPA claim, arguing it was barred due to the notice-and-cure provision. Defendant “claimed to have enhanced its security measures” after receiving notice of the alleged violation, and thus “cured all alleged violations within the requisite time period.”^[426] The court found this straightforward assertion insufficient because “the implementation and maintenance of reasonable security procedures and practices . . . following a breach does not constitute a cure with respect to that breach.”^[427] The court pointed out that the defendant had not provided any additional detail on the nature of its cure, concluding that this was insufficient at the motion-to-dismiss stage.^[428]

e. Guidance on Reasonable Security Measures in Connection with the CCPA In addition to the cases highlighted by [last year's Review](#),^[429] courts have continued to weigh in on what qualifies as reasonable data security measures under the CCPA. **Moving Company.** Plaintiffs brought suit after their personal information was stolen by hackers in a cyberattack. Plaintiffs asserted violations of the CCPA for failure to take reasonable precautions to protect their personal information.^[430] The court declined to dismiss the CCPA claim, and identified a number of measures the defendants could have taken prior to the breach. Plaintiffs specifically alleged that the defendant’s security measures were inadequate because they failed to implement “adequate filtering software,” “adequate[] training,” “multi-factor authentication,” encryption, and destruction when the personal information was no longer in use.^[431] The court also pointed to plaintiff’s complaint, which “identif[ied] fourteen cybersecurity best practices that defendant should have followed but allegedly did not.”^[432] **Large National Bank.** Plaintiffs brought numerous claims arising out of prepaid benefits payment cards issued by the bank.^[433] Plaintiffs alleged that these cards were targeted by bad actors, and the information was easily accessible since the cards had magnetic strips instead of chips. Plaintiffs claimed that erroneous charges and unauthorized transactions resulted in the loss of their funds and alleged violations of the CCPA due to the debit cards’ lack of chip technology, asserting that use of chip technology is a necessary reasonable security measure to protect their personal information. The court agreed, finding that the allegations stated a claim under the CCPA.^[434] The court also found that plaintiffs’ allegation that the bank failed to subject its agents to background checks was adequate to state a claim based on failure to implement and maintain reasonable security measures and practices.^[435]

2. State Biometric Information Litigation

a. Illinois Biometric Information Privacy Act 2023 was another active year for Illinois’s biometrics law, with courts continuing to expand the scope of the Biometric Information Privacy Act (“BIPA”), but also recognizing new limitations. Perhaps unsurprisingly, Illinois also continued as the leading state with respect to biometrics-related litigation.

i. Expansion of BIPA’s Scope

BIPA’s Statute of Limitations Under Section 15. The Supreme Court of Illinois found that claims brought under Section 15 of BIPA (which relates to retention, collection, disclosure, storage, and use of biometric information) have a five-year statute of limitations, reversing an appellate court’s ruling that placed a one-year limit on such claims.^[436] Under Illinois law, “actions . . . to recover damages for an injury done to property, real or personal . . . and all civil actions not otherwise provided for, shall be commenced within 5 years next after the cause of action accrued.”^[437] Part of the court’s justification for finding that the default Illinois statute of limitations five-year catchall applied was because a shorter limit would “thwart [the] legislative intent” of BIPA to provide

redress for persons aggrieved and “shorten the amount of time a private entity would be held liable for noncompliance with the Act.”^[438] Additionally, upon a certified question from the Seventh Circuit, the Supreme Court of Illinois ruled in a 4-3 decision that BIPA claims “accrue under the Act each time a private entity scans or transmits an individual’s biometric identifier or information in violation of section 15(b) or 15(d).”^[439] The court dismissed ongoing policy-based concerns about massive damages by reiterating that the court “has repeatedly recognized the potential for significant damages awards under the Act” and that such high damages operate as an incentive for private entities to conform to state law.^[440] While noting trial courts presiding over a class action “possess the discretion to fashion” a fair yet less-deleterious award, the court concluded that the legislature was the best vehicle to address policy concerns and the plain language of the statute authorized accrual of claims.^[441]

BIPA Claims Survive Death. Also in 2023, a federal court in Illinois, hearing a class action case where the named plaintiff passed away, held that BIPA created a personal property interest and claims survive the plaintiff’s death.^[442]

ii. New Recognized Limitations Under BIPA Even so, courts recognized limitations to claims brought under BIPA in 2023.

“Active Steps” In Furtherance of Collecting Biometric Data. For example, an Illinois federal judge dismissed two claims in a proposed class action where an employer used third-party timekeeping software that registered and scanned employee fingerprints which were then stored on a vendor’s cloud storage service.^[443] The judge held that the cloud storage vendor did not take an “active step” in furtherance of collecting biometric information merely by contracting with the third party to provide access to the vendor’s cloud storage system, but instead was “merely a vendor to the third party that provided the biometric timekeeping technology and services to [the employer].”^[444]

Exceptions to Collections of Biometric Data: In some cases, courts found that certain exceptions privileged the collection of biometric data—for example, one trial court held that the “general health care exemption” to BIPA covered a virtual try-on tool for sunglasses, finding sunglasses to be a Class I medical device under the FDA.^[445] Another court denied the plaintiff’s motion to strike the defendant’s affirmative defense that “the biometric identifiers it collects fall within [the general health care] exception because they are collected along with medical information provided by a donor,” such as fingerprints taken prior to donating plasma used to identify the patient during each donation.^[446] The court noted that BIPA does not define the term “patient” nor does it define the term “health care” and found that the defendant’s arguments as to why the exception applied were sufficient to survive a motion to strike.^[447]

b. Texas Biometric Privacy Law Litigation As discussed in [last year’s Review](#), in February 2022, Texas Attorney General Ken Paxton brought the first enforcement action under the Texas Capture and Use of Biometric Identifier Act (“CUBI”) more than two decades after its passage in 2001.^[448] AG Paxton asserted a CUBI claim against a large social media company alleging that the company’s collection of “facial geometries” in connection with its facial recognition and tagging feature that it deprecated in November 2021 violated CUBI, in addition to bringing claims under Texas’ Deceptive Trade Practices Act.^[449] The parties continued to conduct discovery in the case throughout 2023. In late October 2022, Texas filed a similar action against another large technology company for alleged violations of CUBI.^[450] The case is still in the early stages of discovery. These two cases remain the only actions brought under CUBI. Given the preliminary enforcement efforts by the state of Texas, companies can continue to expect heightened state-level scrutiny and enforcement in the biometrics arena in 2024.

c. New York Biometric Privacy Law Litigation 2023 also saw challenges under the N.Y.C. Biometric Privacy Law. On May 19, 2023, two plaintiffs filed a class action against a large live-entertainment company for its alleged use of facial recognition software to keep banned individuals out of its venues.^[451] The plaintiffs allege that the company collects biometric information from every person who enters its venues, and then compares that information to an internal database of banned individuals.^[452] The complaint further alleges that the company shares this biometric information with at least one third-party vendor, and that the company ultimately benefits in the form of reduced litigation costs.^[453] The plaintiffs allege that this undisclosed collection, use, and disclosure of customers’ biometric data violates the 2021 New York City Biometric Identifier Information Law and the right to privacy guaranteed by Article 5 of the New York Civil Rights Law.^[454] Plaintiffs also pleaded an unjust enrichment claim, maintaining that the company wrongfully obtained

benefits from the proposed plaintiff class in the form of valuable data.^[455] On January 9, 2024, a federal magistrate judge released a report recommending dismissal of the civil rights and unjust enrichment claims.^[456] On the civil rights law claim, the court found that the limitations period of one year had already run for one plaintiff.^[457] For the other plaintiff, the court found that the defendant's alleged collection and use of biometric information to remove banned individuals could not plausibly be understood "as seeking to draw trade at its venues"—a necessary element of a claim under the civil rights statute.^[458] The magistrate also recommended dismissing the unjust enrichment claim on the ground that "New York courts have long recognized the Civil Rights Law as 'preempting all common law claims based on unauthorized use of name, image, or personality, including unjust enrichment claims.'"^[459] Thus, under New York law, there can be no unjust enrichment claim arising from use of one's personal image.^[460] The magistrate recommended allowing the New York City Biometric Identifier Law claim to proceed, finding that the defendant's alleged conduct is consistent with the text and legislative history of the statute.^[461]

F. Other Noteworthy Litigation

Supreme Court Declines to Address Scope of Section 230. In [last year's Review](#), we noted that the U.S. Supreme Court granted certiorari in two cases that could affect the scope of Section 230 of the Communications Decency Act of 1996, which protects "interactive computer services" from liability for user-published content. In each case, *Twitter, Inc. v. Taamneh*^[462] and *Gonzalez v. Google LLC*,^[463] plaintiffs alleged that social media companies were liable under the Anti-Terrorism Act (ATA) for aiding and abetting acts of terrorism that resulted in the deaths of plaintiffs' family members. According to the plaintiffs, ISIS allegedly used the defendants' websites to fundraise and recruit new members, with little interference by content moderators—and sometimes even active promotion by the defendants' algorithms. Both cases came from the Ninth Circuit Court of Appeals, which had allowed the *Taamneh* case to proceed^[464] but held that Section 230 barred most of the claims in *Gonzalez*.^[465] The U.S. Supreme Court unanimously reversed the Ninth Circuit's decision in *Taamneh*, holding that the plaintiffs had not stated a claim under the ATA because they failed to show "any concrete nexus between defendants' services" and the attack.^[466] On the same day, the Court declined to address the Ninth Circuit's holding regarding Section 230 in *Gonzalez*, instead remanding the case for reconsideration in light of *Taamneh*.^[467] Thus the Court effectively sidestepped the question of whether Section 230 bars platform liability for algorithmic amplification of user-published content by resolving one case on ATA grounds alone and remanding the other.

Large Technology Companies Continue to Face VPPA-Related Litigation. Several lawsuits were filed in 2023 concerning companies' collection and management of users' video-related information. For example, with respect to a lawsuit relating to one major technology company's management of user video history information, a federal district court dismissed with prejudice a claim that the company's alleged retention of the plaintiff's video rental history violated the New York Video Consumer Privacy Act and the Minnesota Video Privacy Law.^[468] The court observed that, like the VPPA, these state analogue statutes were meant to prevent unauthorized *disclosure* of video-related data rather than mere retention of it.^[469] In another video-related case,^[470] a federal court held that the plaintiff had adequately pleaded a VPPA violation by alleging that a company disclosed information about the plaintiff's online activity to his school district, which was using the company's platform for digital learning during the COVID-19 pandemic.^[471] The company moved to dismiss this claim on two grounds: First, it argued that the plaintiff was not a "subscriber" within the meaning of the VPPA, since his account with the defendant was a byproduct of his relationship with the school district.^[472] Second, the company argued that any disclosure of PII was permitted by the VPPA because it was done "in the regular course of business" with the school district.^[473] The court rejected both arguments, finding that the plaintiff, who held an account directly with the defendant, was plausibly a subscriber.^[474] The court also said it was not appropriate to decide the second issue at the motion to dismiss stage, as the company's contract with the district was not part of the court's record.^[475]

Employers May Be Potentially Liable for Failing to Secure Employees' Personally Identifiable Information. 2023 also saw new lawsuits focusing on employee data privacy and seeking to hold employers liable for failing to secure employees' PII or failing to implement appropriate safeguards. For example, the United States Court of Appeals for the Eleventh Circuit ruled that a plaintiff had plausibly

alleged a negligence claim against a former employer that failed to protect PII in the employer's possession.^[476] The complaint alleges that as a condition of employment, the plaintiff and members of the proposed class were required to give the defendant certain PII like their names and Social Security numbers.^[477] However, the employer did not maintain adequate security measures to protect that information, and the PII was subsequently leaked in a ransomware attack on the employer's system.^[478] The court held that such an attack was reasonably foreseeable for a large employer like the defendant; that the plaintiff adequately pleaded that the former employer owed him a duty of care; and that failure to comply with standard data security practices was plausibly a breach of that duty.^[479] Thus, the court allowed the plaintiff's negligence claim to move forward. Likewise, a major car manufacturer was sued for allegedly failing to protect the personal information of 75,000 current and former employees that was exposed in a data breach carried out by former employees of the company.^[480] The complaint alleges that the company failed to implement or follow reasonable data security procedures as required by law, and failed to protect the sensitive information of class members from unauthorized action.^[481] The case is in its early stages, and there has not yet been any dispositive-motion practice.

IV. Trends Related to Data Innovations and Governmental Data Collection A. Data-Intensive Technologies—Privacy Implications and Trends

With the continued proliferation of data-intensive technologies, big data processing and its privacy implications continued to be an area of great focus in 2023. In addition to innovations and issues pertaining to AI, which are covered in detail in Gibson Dunn's forthcoming Artificial Intelligence Legal Review, there was a renewed focus on smart cities, edge computing and privacy-enhancing technologies (PETs). **Smart Cities.** The trend over the past decade of cities getting "smarter" continued at a rapid clip in 2023. A "smart city" leverages technology, data-driven decision-making, and digitally connected infrastructure to optimize the quality of municipal services, promote safe and sustainable communities, and achieve operational efficiencies.^[482] Most of the technologies that smart cities are currently using do not collect or process personal data. For example, smart street-lighting technologies allow cities to turn on, turn off, and dim street lights based on the time of day and weather events and smart water management technologies allow cities to detect chemicals in drinking water and wastewater systems.^[483] However, given that smart city technology applications are fueled by and necessitate large scale collection and processing of data as well as government partnership with the private sector, privacy advocates and policy makers are increasingly concerned about the privacy implications of such technology. These concerns largely relate to:

- **Data security:** Smart cities can be vulnerable to cyberattacks because they rely on internet of things ("IoT") devices, which are common and often insecure targets.^[484] Furthermore, local governments often lack the resources to obtain secure technologies, update them, and employ cybersecurity experts.^[485] In fact, a recent survey found that nearly one-third of local governments would be unable to detect whether their systems had been hacked.^[486]
- **Commercial use of data:** Smart city data may be used commercially if a city partners with a private company to pay for technologies and in exchange gives the company access to data the city collects.^[487] A privacy concern arises if the city shares sensitive data with private partners.
- **Government surveillance:** Some privacy advocates are concerned that governments will use smart city technologies to surveil individuals by obtaining data the government could not otherwise compel access to or by pulling data from different sources to build behavior profiles on individual residents.^[488] Critics assert that cities are already theoretically able to aggregate enough data from smart city technologies to build detailed behavior profiles on their residents.^[489] Ultimately, these debates may be settled by courts, which will decide if these data collection practices violate U.S. privacy laws or the Fourth Amendment.^[490]

Although there has not been any legislation seeking to specifically regulate smart city technologies, many of the existing or pending privacy regulations are potentially applicable. However, as smart city technologies, particularly those implicating personal

information or sensitive data, continue to grow in number and capability, we expect to see more specific legislation targeting such technology and use cases. **Edge Computing.** The enormous volume of data being generated and processed by data-intensive technologies—e.g., IoT devices—has strained traditional computing models. This has led organizations to increasingly embrace “edge computing”—an emerging decentralized computing paradigm where data is processed closer to where it is generated, thus allowing processing of greater data volumes at greater speed.^[491] Experts predict that spending on edge technology will continue to soar.^[492] Due to deployment of strong internet infrastructures and a growing awareness of the importance of IoT across industries, the edge computing market is estimated to grow at a compound annual growth rate of 21.6% to hit an estimated \$132.11 billion in 2028.^[493] The number of endpoint devices in use is also expected to skyrocket, with estimates of up to 55.7 billion total IoT devices deployed worldwide in the next few years.^[494] Telecommunication companies are expected to play a large role in the growth of edge computing, as their widespread infrastructure and expansive reach position them well, literally (based on their close physical proximity to potential customers) and figuratively, to tap the edge computing market.^[495] Although the rise of edge computing is largely a function of the benefits to data processing speed and volume, edge computing has important data privacy and security benefits. For example, edge computing can mitigate some of the privacy risks innate to centralized storage and processing.^[496] by diffusing data and thus reducing the scope and impact of a data breach. Edge computing may also reduce the incentives for malicious actors, as an edge device with one or a few users’ data is a less desirable target than a cloud database with millions of users’ data.^[497] However, by the same token, storing and processing data on devices outside of a centralized corporate network potentially makes the data less secure, given that personal edge devices are often less secure than corporate devices.^[498] Some commentators have also suggested that edge computing may be an effective compliance tool, particularly with respect to cross-border data transfer laws. For example, one commentator believes that corporations will be able to use edge computing to manage personal data in adherence with local privacy laws by “placing certain local[iz]ed proxy policies that will not allow certain types of data to leave that legal jurisdiction.”^[499] Traces of this can be found in the EU’s federated cloud infrastructure model, GAIA-X, which aims to let national governments apply local laws to cloud-hosted data.^[500] Given the rapid proliferation of data-intensive technologies, we expect organizations to continue to focus on alternative computing paradigms like edge computing, which will bring new benefits and challenges for data privacy and security. **B. Emerging Privacy Enhancing Technologies (PETs)** In March 2023, the White House Office of Science and Technology Policy (“OSTP”) published its “National Strategy to Advance Privacy-Preserving Data Sharing and Analytics.” In sum, the report and strategy calls for development and implementation of PETs in order to mitigate the privacy risks inherent in, and thus unlock the innovative and economic benefits of, large-scale data processing.^[501] Examples of PETs include:

- *Homomorphic encryption:* Homomorphic encryption is a differential privacy technique (adding noise to the data to prevent an adversary from determining whether any individual’s data was or was not included in the original dataset)^[502] that allows computing over encrypted data to produce results in an encrypted form.^[503] In other words, the data retains its relevant statistical characteristics for analysis, while hiding the data itself.^[504] Then, only authorized users can extract the result from its encrypted format or see the original data.^[505] However, homomorphic encryption is currently somewhat limited by higher computational costs and time.^[506]
- *Secure multi-party computation:* Secure multi-party computation allows several parties to simultaneously perform agreed-upon computations over their data, while permitting each individual entity to learn only the final output.^[507] Accordingly, distributed datasets can be computed over without revealing the source data.^[508] However, the requirement of joint collaboration can lead to higher communication and computational costs, making it difficult to scale.^[509]
- *Federated learning:* Federated learning allows multiple entities to collaborate and

build machine-learning algorithms to process data on edge devices, such as smartphones.[\[510\]](#) Accordingly, the underlying data is not aggregated. Instead, the locally trained models are aggregated in the cloud.[\[511\]](#) In this way, participants do not have to share their raw data, providing inherent privacy protection. However, federated learning has recently been shown to be vulnerable to model inversion attacks.[\[512\]](#) Research into closing these vulnerabilities and creating privacy-preserving federated learning is ongoing.[\[513\]](#)

- *Zero-knowledge proof*: Zero-knowledge proof allows one party, the “prover,” to offer proof to another party, the “verifier,” that a statement is true without revealing any sensitive information.[\[514\]](#) Some digital assets use this technique to prove statements about transactions without revealing additional metadata.[\[515\]](#) and neural networks are using zero-knowledge proof schemes to show that prediction tasks are being carried out, without disclosing any information about the model itself.[\[516\]](#) However, zero-knowledge proof currently has some cost and scalability limitations.[\[517\]](#)

According to the OSTP report, the impetus for a national strategy on PETs is the White House’s belief that large-scale data processing is crucial for innovation and the economy. However, given the complex domestic and international regulatory landscape, the White House recognizes that inherent in such processing are significant privacy risks for data subjects and organization data subjects and organizations.[\[518\]](#) Accordingly, the strategy calls for the adoption of PETs, which can mitigate the privacy risks of large-scale data processing and thus unlock the benefits of data processing to fuel innovation and the economy. The OSTP report enumerates 16 recommendations across five strategic priorities to advance the development and use of PETs.[\[519\]](#) Importantly, the report specifically calls for the use of secure multi-party computation and zero-knowledge proofs, as well as increased public and private sector partnership and U.S.

partnerships/collaboration with foreign governments. In the absence of a comprehensive federal privacy law and/or regulations specifically focused on privacy-preserving technologies, the OSTP’s strategy signifies what may be the beginning of a burgeoning national standard for the development and use of PETs. **C. Governmental Data Collection EU-US Data Privacy Framework.** In July 2023, the European Commission adopted its adequacy decision for the EU-U.S. Data Privacy Framework, concluding that U.S. protection of cross-border data transfers is comparable to the protection offered by the EU.[\[520\]](#) Speaking during a press conference announcing adoption of the U.S. adequacy decision, EU justice commissioner Didier Reynders said, “[w]ith the adoption of the adequacy decision, personal data can now flow freely and safely from the European Economic Area to the United States without any further conditions or authorizations.”[\[521\]](#) The decision resolved the legal uncertainty surrounding exports of EU users’ personal data by U.S. companies that had existed since the Court of Justice of the European Union invalidated the EU-U.S. Privacy Shield in 2020.[\[522\]](#) However, legal challenges are expected, with critics claiming that the Data Privacy Framework merely “paper[s] over the same fundamental legal conflict between EU privacy rights and U.S. surveillance powers.”[\[523\]](#) Nonetheless, Reynders emphasized that the “new framework is substantially different than the EU-U.S. Privacy Shield as a result of the Executive Order issued by President Biden [in 2022]” and highlighted the reworked redress mechanism that will boast “an independent and impartial tribunal that is empowered to investigate complaints lodged by Europeans and to issue binding remedial decisions.”[\[524\]](#) Finally, Reynders cautioned U.S. technology giants that “[i]t will be for the companies to show that they’re in full compliance with the GDPR [General Data Protection Regulation].”[\[525\]](#) On July 17, 2023, the Department of Commerce launched the new Data Privacy Framework program website, dataprivacyframework.gov.[\[526\]](#) The website allows U.S. companies to self-certify their participation in and commitment to the EU-U.S. Data Privacy Framework (“DPF”), and, optionally, the UK Extension or Swiss-U.S. DPF Principles, in order to participate in cross-border transfers of personal data. **Government Surveillance Reform Act (GSRA).** In November 2023, a bipartisan group of senators introduced the Government Surveillance Reform Act (“GSRA”), which would reform the Foreign Intelligence Act (“FISA”) and amend the Electronic Communications Privacy Act

(“ECPA”). Importantly, the GSRA proposes significant restrictions on government surveillance and access to data—including, among other things, (i) protecting Americans from warrantless backdoor searches, (ii) requiring warrants for Americans’ location data, web browsing and search records, and vehicle data, (iii) restricting government collection of Americans’ information as part of large datasets and prohibiting the government from purchasing Americans’ data from data brokers, and (iv) prohibiting the collection of Americans’ domestic communications.^[527] FISA, Section 702 was set to expire at the end of 2023,^[528] but Congress approved a short-term extension in December 2023.^[529] Under Section 702, the government could collect communications by non-Americans located abroad, without a warrant.^[530] However, the private phone calls, emails, and text messages of U.S. persons were captured by the blanket surveillance techniques deployed under Section 702.^[531] In response, several lawmakers vowed not to reauthorize Section 702 without “significant reforms.”^[532] The GSRA would ban officials from conducting searches for Americans’ communications unless they first obtain a warrant in a criminal investigation or a FISA Title I order in a foreign intelligence investigation.^[533] The new warrant requirement would provide for narrow exceptions in cases of: (1) consent, (2) exigent circumstances, or (3) a government attempt to identify targets of cyberattacks by searching for malicious code embedded in Americans’ communications.^[534] The GSRA would also significantly overhaul the ECPA—which addresses wiretapping, access to stored electronic communications, and other information-collection devices.^[535] These changes would alter the rights and obligations of entities already covered by the ECPA and expand the reach of the ECPA to entities not currently subject to it.^[536] The GSRA would:

- Expand the scope of companies subject to the ECPA to include any online service provider.^[537] The GSRA would add a new category of service providers—broadly defined as “any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server”^[538]—to the Stored Communications Act’s (“SCA”) provision governing compelled disclosures to governmental entities.^[539]
- Effectively codify the Sixth Circuit’s decision in *Warshak v. United States*, 631 F.3d 266 (6th Cir. 2010), which held that law enforcement must obtain a warrant to compel the disclosure of the contents of user communications.^[540] Further, the GSRA would effectively codify *Carpenter v. United States*, 138 S. Ct. 2206 (2018), by requiring law enforcement to obtain a warrant to compel the disclosure of location information, web browsing records, online search queries, and covered vehicle data.^[541]
- Prohibit the government from purchasing the personal data of U.S. persons (U.S. citizens and lawful permanent residents) or people reasonably believed to be located inside the United States.^[542]
- Exempt congressional subpoenas from the ECPA, allowing political officials to subpoena the communications and personal data of U.S. persons without any statutory protection.^[543]

Dueling Surveillance Bills in the U.S. House of Representatives. In December 2023, the House postponed a planned vote on two competing surveillance bills under a procedural rule called “Queen of the Hill,” whereby the bill with the most votes is sent to the Senate.^[544] The House Intelligence Committee advanced the first bill, the FISA Reform and Reauthorization Act of 2023, which faced backlash from privacy rights groups.^[545] More than 50 organizations signed a letter demanding the bill’s rejection.^[546] By contrast, the second bill, proposed by the House Judiciary Committee, entitled The Protect Liberty and End Warrantless Surveillance Act, received support from privacy advocates.^[547] Both bills are still pending in the House. **V.**

Conclusion In 2023, the privacy and cybersecurity landscape in the U.S. was defined by an expansion of regulatory and enforcement activity led by federal and state agencies, as well as civil litigation brought by private plaintiffs. This was driven in large part by the rapid development and advances in data-intensive technologies like AI and IoT; the unrelenting

cyber threat posed by malicious actors; and related litigation arising from these trends. We expect these trends to continue in 2024 as existing technologies and use cases take hold and new ones emerge. In the absence of comprehensive federal legislation (which is unlikely in an election year), we expect federal and state agencies to continue to lead the charge on the regulatory front and aggressively pursue enforcement actions against companies and individuals. We will continue to track and analyze these developments in the year ahead. _____ [1] Cal. Civ. Code § 1798.100 *et seq.* [2] Va. Code Ann. §§ 59.1-575 to 59.1-585. [3] Colo. Rev. Stat. Ann. § 6-1-1308. [4] Conn. Gen. Stat. Ann. § 42-520. [5] Utah Code §§ 13-61-101 to 13-61-404. [6] S.B. 262, 125 Reg. Sess. (Fla. 2023) (to be codified in Fla. Stat. § 501.701-22). [7] H.B. 4, 88 Reg. Sess. (Tex. 2023) (to be codified in Tex. Bus. & Com. Code §§ 541.001 to 541.205). [8] S.B. 618, 82 Leg. Assemb., Reg. Sess. (Or. 2023) (to be codified in Or. Laws Ch. 369). [9] S.B. 384, 68 Reg. Sess. (Mont. 2023) (to be codified in Mont. Code § 30-14-2801 to 30-14-2817). [10] S.F. 262, 89th Gen. Assemb., Reg. Sess. (Iowa 2023) (to be codified in Iowa Code § 715D.1 to 715D.9). [11] H.B. 154, 152 Gen. Assemb., Reg. Sess. (Del. 2023) (to be codified in 6 Del. Code § 12D). [12] S.B. 332, 220 Leg. Assemb., Reg. Sess. (N.J. 2023). [13] H.B. 1181; S.B. 73, 112 Gen. Assemb., Reg. Sess. (Tenn. 2023) (to be codified in Tenn. Code §§ 47-18-3301 to 47-18-3315). [14] S.B. 5, 123 Gen. Assemb., Reg. Sess. (Ind. 2023) (to be codified in Ind. Code §§ 24-15-1-1 to 24-15-11-2). [15] Notably, under the NJDPA, “financial information” is included as a form of sensitive data, which is defined as including “a consumer’s account number, account log-in, financial account, or credit or debit number, in combination in combination with any required security code, access code, or password that would permit access to a consumer’s financial account.” [16] Under Civil Code section 1798.150, the damages available for a private right of action to pursue statutory damages between \$100 and \$750 per consumer per incident or actual damages, whichever is greater, as well as injunctive or declaratory relief, and “any other relief the court deems proper.” A number of limitations also exist. For example, under Section 1798.150(b), a consumer must give a business an opportunity to “cure” the alleged violation by sending written notice prior to filing suit. If cured within 30 days and the consumer receives “an express written statement” indicating that the violations have been cured and shall not recur, a claim for statutory damages cannot be pursued. [17] *Protecting Washingtonians’ Personal Health Data and Privacy*, Wash. Att’y Gen., <https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy>. [18] Wash. Rev. Code § 19.373.010(23). [19] *Id.* § 19.373.010(23). [20] *Id.* §§ 19.373.010(28), 19.373.030(2). [21] *Id.* § 19.373.010(8)(a). [22] *Id.* § 19.373.010(8)(b). [23] *Id.* § 19.373.010(8)(c). [24] *Id.* [25] *Protecting Washingtonians’ Personal Health Data and Privacy*, Wash. Att’y Gen., <https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy>. [26] Wash. Rev. Code §§ 19.373.020; 19.373.030. [27] *Id.* §§ 19.373.010(6)(a); 19.373.030. [28] *Id.* § 19.373.040(a)–(c). [29] *Id.* § 19.373.090. [30] *Id.* § 19.255.040. [31] *Id.* [32] Mont. Code § 30-23-102(4). [33] *Id.* § 30-23-102(6). [34] *Id.* § 30-23-104(1)–(2). [35] *Id.* § 330-23-104(5). [36] *Id.* § 30-23-106. [37] Press Release, Senator Josh Becker, *Governor Newsom Signs First in the Nation Bill to Protect Consumers’ Data from Unknown Third Parties* (Oct. 10, 2023), <https://sd13.senate.ca.gov/news/press-release/october-10-2023/governor-newsom-signs-first-in-the-nation-bill-to-protect>. [38] Cal. Civ. Code §§ 1798.99.84; 1798.99.86(a)–(b). [39] *Id.* § 1798.99.86(c)–(d). [40] *Id.* § 1798.99.86(d)(2). [41] *Id.* § 1798.99.86(a)(3). [42] *Id.* § 1798.99.86(e)(1). [43] *Id.* § 1798.99.80(c). [44] *Id.* § 1798.99.80(c)(1)(4). [45] N.Y. Dep’t of Fin. Servs., *Cybersecurity Resource Center*, https://www.dfs.ny.gov/industry_guidance/cybersecurity. [46] N.Y. Dep’t of Fin. Servs., *Enforcement and Discipline*, https://dfs.ny.gov/industry_guidance/enforcement_actions. [47] Press Release, Utah Governor Spencer J. Cox, *Cox Signs Bills Focused on Social Media and Youth Mental Health in Utah* (Mar. 23, 2023), <https://governor.utah.gov/2023/03/23/gov-cox-signs-bills-focused-on-social-media-in-utah/>. [48] Utah Code § 13-63-101, *et seq.* [49] *Id.* §§ 13-63-201–301. [50] *Id.* § 13-63-301. [51] *NetChoice, LLC v. Reyes*, No. 2:23-cv-00911 (D. Utah); *Zoulek v. Hass*, No. 2:24-cv-00031 (D. Utah). [52] *NetChoice, LLC v. Griffin*, No. 5:23-CV-05105, 2023 WL 5660155, at *7 (W.D. Ark. Aug. 31, 2023). [53] *Id.* at *13. [54] *Id.* at *17, 40–41. [55] *Alario v. Knudsen*, No. CV 23-56-M-DWM, 2023 WL 8270811 (D. Mont. Nov. 30, 2023). [56] *Id.* at *4. [57] American Data Privacy and Protection Act (“ADPPA”),

GIBSON DUNN

H.R. 8152, 117th Cong. (2022). [58] *Id.* §§ 101(a)–(b), 103(a). [59] *Id.* § 207(a)(1). [60] *Id.* §§ 207(b), 401, 402(a). [61] *Id.* § 403(a). [62] *Id.* § 404(b)(1). [63] See *Innovation, Data, and Commerce Subcommittee Hearing: “Addressing America’s Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans’ Personal Information,”* U.S. House Energy & Commerce Comm. (Apr. 27, 2023), <https://energycommerce.house.gov/events/innovation-data-and-commerce-subcommittee-hearing-addressing-america-s-data-privacy-shortfalls-how-a-national-standard-fills-gaps-to-protect-americans-personal-information>; *Innovation, Data, and Commerce Subcommittee Hearing: “Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy,”* U.S. House Energy & Commerce Comm. (Mar. 1, 2023), <https://energycommerce.house.gov/events/innovation-data-and-commerce-subcommittee-hearing-promoting-u-s-innovation-and-individual-liberty-through-a-national-standard-for-data-privacy>. [64] Exec. Order No. 14,110, 88 Fed. Reg. 75191 (Oct. 30, 2023); see also Press Release, White House, *FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence* (Oct. 30, 2023), <https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence>. [65] Remarks of President Joe Biden – *State of the Union Address as Prepared for Delivery*, White House (Feb. 7, 2023), <https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/02/07/remarks-of-president-joe-biden-state-of-the-union-address-as-prepared-for-delivery>. [66] See Eric McDaniel, *Congress Passed So Few Laws This Year That We Explained Them All in 1,000 Words*, NPR (Dec. 22, 2023), <https://www.npr.org/2023/12/22/1220111009/congress-passed-so-few-laws-this-year-that-we-explained-them-all-in-1-000-words>; Müge Fazlioglu, *US Federal Privacy Legislation Tracker: Introduced in the 118th Congress (2023-2024)*, IAPP (last updated Sept. 2023), https://iapp.org/media/pdf/resource_center/us_federal_privacy_legislation_tracker.pdf. [67] Müge Fazlioglu, *U.S. Privacy Legislation in 2023: Something Old, Something New?*, IAPP (July 26, 2023), <https://iapp.org/news/a/u-s-federal-privacy-legislation-in-2023-something-old-something-new>. [68] Press Release, U.S. Senate Judiciary Comm., *Durbin, Graham Announce January 2024 Hearing with Five Big Tech CEOs on their Failure to Protect Children Online* (Nov. 29, 2023), <https://www.judiciary.senate.gov/press/releases/durbin-graham-announce-january-2024-hearing-with-five-big-tech-ceos-on-their-failure-to-protect-children-online>; *Full Committee Hearing: “TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms,”* U.S. House Energy & Commerce Comm. (Mar. 23, 2023), <https://energycommerce.house.gov/events/full-committee-hearing-tik-tok-how-congress-can-safeguard-american-data-privacy-and-protect-children-from-online-harms>. [69] Kids Online Safety Act, S. 1409, 118th Cong. (2023). [70] Children and Teens’ Online Privacy Protection Act, S. 1418, 118th Cong. (2023). [71] Informing Consumers about Smart Devices Act, S. 90, 118th Cong. (2023). [72] Stop Spying Bosses Act, S. 262, 118th Cong. (2023). [73] UPHOLD Privacy Act of 2023, S. 631, 118th Cong. (2023). [74] DELETE Act, H.R. 4311, 118th Cong. (2023). [75] Data Care Act of 2023, S. 744, 118th Cong. (2023). [76] Online Privacy Act of 2023, H.R. 2701, 118th Cong. (2023). [77] Federal Cybersecurity Vulnerability Reduction Act of 2023, H.R. 5255, 118th Cong. (2023). [78] Modernizing the Acquisition of Cybersecurity Experts Act of 2023, H.R. 4502, 118th Cong. (2023). [79] Federal Cybersecurity Workforce Expansion Act, S. 2256, 118th Cong. (2023). [80] See Press Release, White House, *President Biden Recognizes Actions by Private Sector Ticketing and Travel Companies to Eliminate Hidden Junk Fees and Provide Millions of Customers with Transparent Pricing* (June 15, 2023), <https://www.whitehouse.gov/briefing-room/statements-releases/2023/06/15/president-biden-recognizes-actions-by-private-sector-ticketing-and-travel-companies-to-eliminate-hidden-junk-fees-and-provide-millions-of-customers-with-transparent-pricing/>. See also Press Release, White House, *FACT SHEET: Executive Order on Promoting Competition in the American Economy* (July 9, 2021), <https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/09/fact-sheet-executive-order-on-promoting-competition-in-the-american-economy/>. [81] Trade Regulation Rule on Unfair or Deceptive Fees, 88 Fed. Reg. 77420 (Nov. 9, 2023), <https://www.federalregister.gov/documents/2023/11/09/2023-24234/trade-regulation-rule->

GIBSON DUNN

[on-unfair-or-deceptive-fees](#); Trade Regulation Rule on Unfair or Deceptive Fees, 89 Fed. Reg. 38 (Jan. 2, 2024). [82] Christine Wilson, *Letter to President Joseph R. Biden* (Mar. 2, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/p180200wilsonresignationletter.pdf. [83] See Press Release, White House, *President Biden Announces Nominees to Bipartisan Boards and Commissions* (July 3, 2023), <https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/03/president-biden-announces-nominees-to-bipartisan-boards-and-commissions>. [84] Melissa Holyoak, Statement Before the U.S. Senate Committee on Commerce, Science, and Transportation (Sep. 20, 2023), <https://www.commerce.senate.gov/services/files/51CBECA7-1810-4CCD-8046-0AE99CA34CC4>. [85] Hawley Holds Nominees, Calls for Further Evaluation of McConnell Nominees, Senate Office of Josh Hawley (Dec. 20, 2023), <https://www.hawley.senate.gov/hawley-holds-nominees-calls-further-evaluation-mcconnell-nominees>. [86] Lina Khan, *Lina Khan: We Must Regulate A.I. Here's How*, New York Times (May 3, 2023), <https://www.nytimes.com/2023/05/03/opinion/ai-lina-khan-ftc-technology.html>. [87] Michael Atleson, *Keep Your AI Claims in Check*, Federal Trade Commission (Feb. 27, 2023), <https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check>. [88] Michael Atleson, *Chatbots, Deepfakes, and Voice Clones: AI Deception for Sale*, Federal Trade Commission (Mar. 20, 2023), <https://www.ftc.gov/business-guidance/blog/2023/03/chatbots-deepfakes-voice-clones-ai-deception-sale>. [89] *Id.* [90] *Id.* [91] Michael Atleson, *The Luring Test: AI and the Engineering of Consumer Trust*, Federal Trade Commission (May 1, 2023), <https://www.ftc.gov/business-guidance/blog/2023/05/luring-test-ai-engineering-consumer-trust>. [92] Michael Atleson, *Watching the Detectives: Suspicious Marketing Claims for Tools that Spot AI-Generated Content*, Federal Trade Commission (May 1, 2023), <https://www.ftc.gov/business-guidance/blog/2023/07/watching-detectives-suspicious-marketing-claims-tools-spot-ai-generated-content>. [93] Alex Gaynor, *Security Principles: Addressing Underlying Causes of Risk in Complex Systems*, Federal Trade Commission (February 1, 2023), <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/security-principles-addressing-underlying-causes-risk-complex-systems>. [94] *Id.* [95] *Id.* [96] Samuel Levine, Chief, Federal Trade Commission, *Remarks of Chief Samuel Levine at the Consumer Data Industry Association Law and Industry Conference* (September 21, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/cdia-sam-levine-9-21-2023.pdf. [97] Mike Swift, *US FTC still pondering 'commercial surveillance' rulemaking, Slaughter tells tech industry*, MLex (Jan. 10, 2024), <https://content.mlex.com/#/content/1535579>. [98] Press Release, Federal Trade Commission, *FTC Finalizes Order Requiring Fortnite maker Epic Games to Pay \$245 Million for Tricking Users into Making Unwanted Charges* (Mar. 14, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-finalizes-order-requiring-fortnite-maker-epic-games-pay-245-million-tricking-users-making>. [99] 15 U.S.C. § 45(a). [100] Complaint, *FTC v. Ring LLC*, Case No. 1:23-cv-1549 (May 31, 2023). [101] Proposed Stipulated Order, *FTC v. Ring LLC*, Case No. 1:23-cv-1549 (May 31, 2023); Press Release, Federal Trade Commission, *FTC Says Ring Employees Illegally Surveilled Customers, Failed to Stop Hackers from Taking Control of Users' Cameras* (May 31, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ring-employees-illegally-surveilled-customers-failed-stop-hackers-taking-control-users>. [102] Notices of Penalty Offenses, Federal Trade Commission, <https://www.ftc.gov/enforcement/penalty-offenses>. [103] Press Release, Federal Trade Commission, *FTC Warns Tax Preparation Companies About Misuse of Consumer Data* (Sep. 18, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/09/ftc-warns-tax-preparation-companies-about-misuse-consumer-data>. [104] Complaint, *U.S. v. Amazon.com, Inc., and Amazon.com Services LLC*, Case No. 2:23-cv-00811 (May 31, 2023). [105] *Amazon Alexa*, Federal Trade Commission (July 21, 2023), <https://www.ftc.gov/legal-library/browse/cases-proceedings/amazon-alexa>. [106] Press Release, Federal Trade Commission, *FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising* (Feb. 1, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising>. [107] Press Release, Federal Trade Commission, *FTC Warns Health Apps and Connected Device Companies to*

GIBSON DUNN

Comply With Health Breach Notification Rule (Sep. 21, 2023), <https://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-warns-health-apps-connected-device-companies-comply-health-breach-notification-rule>. [108] Press Release, Federal Trade Commission, *FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising* (Feb. 1, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising>. [109] Health Breach Notification Rule, 88 Fed. Reg. 37819, 37839 (June 9, 2023), <https://www.federalregister.gov/documents/2023/06/09/2023-12148/health-breach-notification-rule>; see also Press Release, Federal Trade Commission, *FTC Proposes Amendments to Strengthen and Modernize the Health Breach Notification Rule* (May 18, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-proposes-amendments-strengthen-modernize-health-breach-notification-rule>. [110] Press Release, Federal Trade Commission, *FTC Finalizes Order with 1Health.io Over Charges it Failed to Protect Privacy and Security of DNA Data and Unfairly Changed its Privacy Policy* (Sep. 7, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/09/ftc-finalizes-order-1healthio-over-charges-it-failed-protect-privacy-security-dna-data-unfairly>. [111] *FTC v. Rite Aid Corp.*, No. 2:23-cv-05023 (E.D. Pa. Dec. 19, 2023). [112] Press Release, Federal Trade Commission, *FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches* (Oct. 27, 2021), <https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial-information-following-widespread-data>. [113] Press Release, Federal Trade Commission, *FTC Amends Safeguards Rule to Require Non-Banking Financial Institutions to Report Data Security Breaches* (October 27, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/10/ftc-amends-safeguards-rule-require-non-banking-financial-institutions-report-data-security-breaches>. [114] Press Release, Federal Trade Commission, *Compliance deadline for certain revised FTC Safeguards Rule provisions extended to June 2023* (November 15, 2022), <https://www.ftc.gov/business-guidance/blog/2022/11/compliance-deadline-certain-revised-ftc-safeguards-rule-provisions-extended-june-2023>. [115] *Id.* [116] Press Release, Federal Trade Commission, *FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches* (Oct. 27, 2021), <https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial-information-following-widespread-data>. [117] Press Release, Federal Trade Commission, *FTC Proposes Strengthening Children's Privacy Rule to Further Limit Companies' Ability to Monetize Children's Data* (December 20, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/12/ftc-proposes-strengthening-childrens-privacy-rule-further-limit-companies-ability-monetize-childrens>. [118] *Id.* [119] *Id.* [120] *Id.*; Children's Online Privacy Protection Rule, 89 Fed. Reg. 2034 (Jan. 11, 2024), <https://www.federalregister.gov/documents/2024/01/11/2023-28569/childrens-online-privacy-protection-rule>. [121] Press Release, Federal Trade Commission, *FTC Seeks Comment on New Parental Consent Mechanism Under COPPA* (July 19, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-seeks-comment-new-parental-consent-mechanism-under-coppa>. [122] *Id.* [123] Press Release, Federal Trade Commission, *FTC Will Require Microsoft to Pay \$20 million over Charges it Illegally Collected Personal Information from Children without Their Parents' Consent* (June 5, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-will-require-microsoft-pay-20-million-over-charges-it-illegally-collected-personal-information>. [124] *Id.* [125] Press Release, Federal Trade Commission, *FTC Proposes Blanket Prohibition Preventing Facebook from Monetizing Youth Data* (May 3, 2023) <https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-proposes-blanket-prohibition-preventing-facebook-monetizing-youth-data>. [126] *Id.* [127] *Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act*, Federal Trade Commission (May 18, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf. [128] Press Release, Federal Trade Commission, *FTC to Host Identity Authentication Workshop* (Feb. 21, 2007) <https://www.ftc.gov/news-events/news/press-releases/2007/02/ftc-host-identity-authentication-w>; *You Don't Say: An FTC Workshop on Voice Cloning Technologies*,

GIBSON DUNN

Federal Trade Commission (Jan. 28, 2020), <https://www.ftc.gov/newsevents/events/2020/01/you-dont-say-ftc-workshop-voice-cloning-technologies>; *Face Facts: A Forum on Facial Recognition Technology*, Federal Trade Commission (Dec. 8, 2011), <https://www.ftc.gov/newsevents/events/2011/12/face-facts-forum-facial-recognition-technology>; *Facing Facts: Best Practices for Common Uses of Facial Recognition Technology*, Federal Trade Commission (Oct. 2012), <https://www.ftc.gov/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies>. [129] *Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act*, Federal Trade Commission (May 18, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf. [130] *Id.* [131] Press Release, Federal Trade Commission, *Rite Aid Banned From Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards* (Dec. 19, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without>. [132] Press Release, Consumer Financial Protection Bureau, *CFPB Proposes Rule to Jumpstart Competition and Accelerate Shift to Open Banking* (Oct. 19, 2023), <https://www.consumerfinance.gov/about-us/newsroom/cfpb-proposes-rule-to-jumpstart-competition-and-accelerate-shift-to-open-banking/>. [133] *Id.* [134] See *id.*; Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796, 74809 (Oct. 31, 2023) (to be codified at 12 C.F.R. pts. 1001, 1033), <https://www.federalregister.gov/documents/2023/10/31/2023-23576/required-rulemaking-on-personal-financial-data-rights>. [135] Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796, 74796 (Oct. 31, 2023) (to be codified at 12 C.F.R. pts. 1001, 1033), <https://www.federalregister.gov/documents/2023/10/31/2023-23576/required-rulemaking-on-personal-financial-data-rights>. [136] 12 U.S.C. § 5533(a). [137] Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796, 74803 (Oct. 31, 2023) (to be codified at 12 C.F.R. pts. 1001, 1033), <https://www.federalregister.gov/documents/2023/10/31/2023-23576/required-rulemaking-on-personal-financial-data-rights>. [138] *Id.* at 74809. [139] *Id.* at 74832. [140] *Id.* at 74833. [141] *Id.* at 74874. [142] *Id.*; Press Release, Consumer Financial Protection Bureau, *Prepared Remarks of CFPB Director Rohit Chopra on the Proposed Personal Financial Data Rights Rule* (Oct. 19, 2023), <https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-of-cfpb-director-rohit-chopra-on-the-proposed-personal-financial-data-rights-rule/>. [143] Press Release, Consumer Financial Protection Bureau, *CFPB Proposes New Federal Oversight of Big Tech Companies and Other Providers of Digital Wallets and Payment Apps* (Nov. 7, 2023), <https://www.consumerfinance.gov/about-us/newsroom/cfpb-proposes-new-federal-oversight-of-big-tech-companies-and-other-providers-of-digital-wallets-and-payment-apps/>. [144] Defining Larger Participants of a Market for General-Use Digital Consumer Payment Applications, 88 Fed. Reg. 80197, 80199, 80204 (Nov. 17, 2023) (to be codified at 12 C.F.R. pt. 1090), <https://www.federalregister.gov/documents/2023/11/17/2023-24978/defining-larger-participants-of-a-market-for-general-use-digital-consumer-payment-applications>. [145] Press Release, Consumer Financial Protection Bureau, *CFPB Proposes New Federal Oversight of Big Tech Companies and Other Providers of Digital Wallets and Payment Apps* (Nov. 7, 2023), <https://www.consumerfinance.gov/about-us/newsroom/cfpb-proposes-new-federal-oversight-of-big-tech-companies-and-other-providers-of-digital-wallets-and-payment-apps/>. [146] *Id.* [147] Press Release, Consumer Financial Protection Bureau, *CFPB Launches Inquiry Into the Business Practices of Data Brokers* (Mar. 15, 2023), <https://www.consumerfinance.gov/about-us/newsroom/cfpb-launches-inquiry-into-the-business-practices-of-data-brokers/>. [148] Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information, 88 Fed. Reg. 16951, 16952 (Mar. 21, 2023), <https://www.federalregister.gov/documents/2023/03/21/2023-05670/request-for-information-regarding-data-brokers-and-other-business-practices-involving-the-collection>. [149] Press Release, Consumer Financial Protection Bureau, *Remarks of CFPB Director*

GIBSON DUNN

Rohit Chopra at White House Roundtable on Protecting Americans from Harmful Data Broker Practices (Aug. 15, 2023), <https://www.consumerfinance.gov/about-us/newsroom/remarks-of-cfpb-director-rohit-chopra-at-white-house-roundtable-on-protecting-americans-from-harmful-data-broker-practices/>. [150] *Id.*; see also 15 U.S.C. § 1681b. [151] *Id.* [152] *Id.* [153] Press Release, Consumer Financial Protection Bureau, *CFPB and Federal Partners Confirm Automated Systems and Advanced Technology Not an Excuse for Lawbreaking Behavior* (Apr. 25, 2023), <https://www.consumerfinance.gov/about-us/newsroom/cfpb-federal-partners-confirm-automated-systems-advanced-technology-not-an-excuse-for-lawbreaking-behavior/>. [154] Press Release, Consumer Financial Protection Bureau, *CFPB Issue Spotlight Analyzes “Artificial Intelligence” Chatbots in Banking* (June 3, 2023), <https://www.consumerfinance.gov/about-us/newsroom/cfpb-issue-spotlight-analyzes-artificial-intelligence-chatbots-in-banking/>. [155] Rohit Chopra, *Algorithms, Artificial Intelligence, and Fairness in Home Appraisals*, CFPB Blog (June 1, 2023), <https://www.consumerfinance.gov/about-us/blog/algorithms-artificial-intelligence-fairness-in-home-appraisals/>. [156] Quality Control Standards for Automated Valuation Models, 88 Fed. Reg. 40638, 40638 (June 21, 2023), <https://www.federalregister.gov/documents/2023/06/21/2023-12187/quality-control-standards-for-automated-valuation-models>. [157] Rohit Chopra, *Algorithms, Artificial Intelligence, and Fairness in Home Appraisals*, CFPB Blog (June 1, 2023), <https://www.consumerfinance.gov/about-us/blog/algorithms-artificial-intelligence-fairness-in-home-appraisals/>. [158] Quality Control Standards for Automated Valuation Models, 88 Fed. Reg. 40638, 40638 (June 21, 2023), <https://www.federalregister.gov/documents/2023/06/21/2023-12187/quality-control-standards-for-automated-valuation-models>. [159] Press Release, Consumer Financial Protection Bureau, *CFPB Issues Guidance on Credit Denials by Lenders Using Artificial Intelligence* (Sept. 19, 2023), <https://www.consumerfinance.gov/about-us/newsroom/cfpb-issues-guidance-on-credit-denials-by-lenders-using-artificial-intelligence/>. [160] *Id.* [161] Press Release, SEC, *SEC Proposes Changes to Reg S-P to Enhance Protection of Customer Information* (Mar. 15, 2023), <https://www.sec.gov/news/press-release/2023-51>. [162] *Id.* [163] *Id.* [164] *Id.* [165] A Small Entity Compliance Guide, SEC, *Cybersecurity Risk Management Strategy, Governance, and Incident Disclosure* (Nov. 14, 2023), https://www.sec.gov/corpfin/secg-cybersecurity#_ftn1. [166] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Exchange Act Release, 88 Fed. Reg. 51896, 51899. [167] *Id.* [168] *Id.* [169] *Id.* [170] *Id.* at 51924. [171] *Id.* at 51898–51899. [172] *Id.* at 51945. [173] *Id.* at 51909–51910. [174] The rule also includes another exemption that only applies to companies subject to the Federal Communications (“FCC”) notification rule for breaches of customer proprietary network information (“CPNI”). A more detailed description of this exception is outlined in Gibson Dunn’s July 31, 2023 update. [175] *Id.* [176] DOJ, *Department of Justice Material Cybersecurity Incident Delay Determinations* (Dec. 12, 2023), <https://www.justice.gov/media/1328226/dl?inline>. [177] *Id.* [178] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Exchange Act Release, 88 Fed. Reg. 51896, 51899. [179] *Id.* [180] *Id.* at 51913. [181] *Id.* [182] *Id.* [183] *Id.* at 51914. [184] The Commission’s Privacy Act Regulations, 88 Fed. Reg. 65807, 65808. [185] *Id.* at 65808–09. [186] Press Release, SEC, *SEC Proposes Cybersecurity Risk Management Rules and Amendments for Registered Investment Advisers and Funds* (Feb. 9, 2022), <https://www.sec.gov/news/press-release/2022-20>. [187] *Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies*, 87 Fed. Reg. 13524 (published Mar. 9, 2022) (to be codified at 17 C.F.R. pts. 230, 232, 239, 270, 274, 275, 279), <https://www.federalregister.gov/documents/2022/03/09/2022-03145/cybersecurity-risk-management-for-investment-advisers-registered-investment-companies-and-business>. [188] SEC, *Agency Rule List - Fall 2023*, https://www.reginfo.gov/public/do/eAgencyMain?operation=OPERATION_GET_AGENCY_RULE_LIST¤tPub=true&agencyCode=&showStage=active&agencyCd=3235&csrf_token=28A8C6498A23E2932F2D7BB0618F4AA9746D20D66D0F1500674B7BEBFD26693FEF119AEDE913D6851EE65F43B418CC81FFA8. [189] SEC, *View Rule* (last visited, Jan. 26, 2023),

GIBSON DUNN

<https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202310&RIN=3235-AN15>. [190] SEC, *2024 Examination Priorities* (Oct. 16, 2023), <https://www.sec.gov/files/2024-exam-priorities.pdf>. [191] Press Release, SEC, *SEC Division of Examinations Announces 2024 Priorities*, <https://www.sec.gov/news/press-release/2023-222/>. [192] SEC, *SEC Enforcement Results for FY23* (last modified, Jan. 22, 2024), <https://www.sec.gov/newsroom/enforcement-results-fy23>. [193] SEC, *SEC Enforcement Results for FY23* (last modified, Jan. 22, 2024), <https://www.sec.gov/newsroom/enforcement-results-fy23>. [194] *Id.* [195] *Id.* [196] Press Release, SEC, *SEC Charges Virtu for False and Misleading Disclosures Relating to Information Barriers* (September 12, 2023), <https://www.sec.gov/news/press-release/2023-176>. [197] *Id.* [198] *Id.* [199] *Id.* [200] Press Release, SEC, *SEC Charges Software Company Blackbaud Inc. for Misleading Disclosures About Ransomware Attack That Impacted Charitable Donors* (March 9, 2023), <https://www.sec.gov/news/press-release/2023-48>. [201] *Id.* [202] *Id.* [203] *Id.* [204] *Id.* [205] Press Release, SEC, *SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures* (Oct. 30, 2023), <https://www.sec.gov/news/press-release/2023-227/>; see also Complaint ¶ 1, *SEC v. SolarWinds Corp.*, No. 1:23-9518 (S.D.N.Y. Oct. 30, 2023), ECF No. 1. [206] Press Release, SEC, *SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures* (Oct. 30, 2023), <https://www.sec.gov/news/press-release/2023-227>. [207] *Id.* [208] *Id.* [209] *Id.* [210] *Id.* [211] *Id.* [212] *Id.* [213] *Id.* [214] *Id.* [215] Press Release, Department of Health and Human Services, *HHS Announces New Divisions Within the Office for Civil Rights to Better Address Growing Need of Enforcement in Recent Years* (Feb. 27, 2023), <https://www.hhs.gov/about/news/2023/02/27/hhs-announces-new-divisions-within-office-civil-rights-better-address-growing-need-enforcement-recent-years.html>. [216] *Id.* [217] *Id.* [218] *Id.* [219] Press Release, Department of Health and Human Services, *HHS Finalizes Rule to Advance Health IT Interoperability and Algorithm Transparency* (Dec. 13, 2023), <https://www.hhs.gov/about/news/2023/12/13/hhs-finalizes-rule-to-advance-health-it-interoperability-and-algorithm-transparency.html>; see also Press Release, Department of Health and Human Services, *HHS Proposes New Rule to Further Implement the 21st Century Cures Act* (Apr. 11, 2023), <https://www.hhs.gov/about/news/2023/04/11/hhs-propose-new-rule-to-further-implement-the-21st-century-cures-act.html>. [220] *Id.* [221] Office of the National Coordinator for Health Information Technology, Department of Health and Human Services, *Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing*, 45 C.F.R. § 170, <https://www.federalregister.gov/documents/2024/01/09/2023-28857/health-data-technology-and-interoperability-certification-program-updates-algorithm-transparency-and>. [222] *Id.*; see also Department of Health and Human Services, *Telehealth policy updates* (Nov. 9, 2023), <https://telehealth.hhs.gov/providers/telehealth-policy/telehealth-policy-updates>. [223] Press Release, Department of Health and Human Services, *Fact Sheet: End of the COVID-19 Public Health Emergency* (May 9, 2023), <https://www.hhs.gov/about/news/2023/05/09/fact-sheet-end-of-the-covid-19-public-health-emergency.html>. [224] *Id.* [225] Department of Health and Human Services, *Telehealth Policy Changes After the COVID-19 Public Health Emergency* (Dec. 19, 2023), <https://telehealth.hhs.gov/providers/telehealth-policy/policy-changes-after-the-covid-19-public-health-emergency>. [226] Press Release, Department of Health and Human Services, *HHS Office for Civil Rights and the Federal Trade Commission Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies* (July 20, 2023), <https://www.hhs.gov/about/news/2023/07/20/hhs-office-civil-rights-federal-trade-commission-warn-hospital-systems-telehealth-providers-privacy-security-risks-online-tracking-technologies.html>. [227] *Id.* [228] FTC, *Updated FTC-HHS publication outlines privacy and security laws and rules that impact consumer health data* (Sept. 15, 2023), <https://www.ftc.gov/business-guidance/blog/2023/09/updated-ftc-hhs-publication-outlines-privacy-security-laws-rules-impact-consumer-health-data>. [229] Press Release, Department of Health and Human Services, *Statement from Secretary Becerra on the One Year Anniversary of the Dobbs v. Jackson Women’s Health Organization Decision* (June

GIBSON DUNN

24, 2023), <https://www.hhs.gov/about/news/2023/06/24/statement-secretary-becerra-one-year-anniversary-dobbs-v-jackson-womens-health-organization-decision.html>. [230] See *Dobbs v. Jackson Women's Health Org.*, 597 U.S. 215 (2022). [231] Press Release, Department of Health and Human Services, *Statement from Secretary Becerra on the One Year Anniversary of the Dobbs v. Jackson Women's Health Organization Decision* (June 24, 2023), <https://www.hhs.gov/about/news/2023/06/24/statement-secretary-becerra-one-year-anniversary-dobbs-v-jackson-womens-health-organization-decision.html>. [232] Press Release, Department of Health and Human Services, *HHS Proposes Measures to Bolster Patient-Provider Confidentiality Around Reproductive Health Care* (Apr. 12, 2023), <https://www.hhs.gov/about/news/2023/04/12/hhs-proposes-measures-bolster-patient-provider-confidentiality-around-reproductive-health-care.html>. [233] *Id.*; see also Regulatory Initiatives, Department of Health and Human Services, *HIPAA Privacy Rule and Reproductive Health Care* (Apr. 14, 2023), <https://www.hhs.gov/hipaa/for-professionals/regulatory-initiatives/index.html>. [234] HIPAA Privacy Rule To Support Reproductive Health Care Privacy, 88 Fed. Reg. 23506 (proposed Apr. 17, 2023) (to be codified at 45 C.F.R. pts. 160, 164); HHS/OCR, *View Rule* (last visited Jan. 26, 2024), <https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202310&RIN=0945-AA20>. [235] Press Release, Department of Health and Human Services, *HHS' Office for Civil Rights Settles HIPAA Investigation of St. Joseph's Medical Center for Disclosure of Patients' Protected Health Information to a News Reporter* (Nov. 20, 2023), <https://www.hhs.gov/about/news/2023/11/20/hhs-office-civil-rights-settles-hipaa-investigati-on-st-josephs-medical-center-disclosure-patients-protected-health-information-news-reporter.html>; Department of Health and Human Services, *St. Joseph's Medical Center Resolution Agreement and Corrective Action Plan* (Aug. 22, 2023), <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/sjmc-racap/index.html>. [236] *Id.* [237] *Id.* [238] *Id.* [239] Press Release, Department of Health and Human Services, *HHS' Office for Civil Rights Settles Multiple HIPAA Complaints With Optum Medical Care Over Patient Access to Records* (Dec. 15, 2023), <https://www.hhs.gov/about/news/2023/12/15/hhs-office-for-civil-rights-settles-multiple-hipaa-complaints-with-optum-medical-care-over-patient-access-to-records.html>. [240] *Id.* [241] See *id.* [242] Press Release, Department of Health and Human Services, *HHS Office for Civil Rights Settles HIPAA Investigation with Arizona Hospital System Following Cybersecurity Hacking* (Feb. 2, 2023), <https://www.hhs.gov/about/news/2023/02/02/hhs-office-for-civil-rights-settles-hipaa-investigation-with-arizona-hospital-system.html>. [243] *Id.* [244] Press Release, Department of Health and Human Services, *HHS' Office for Civil Rights Settles First Ever Phishing Cyber-Attack Investigation* (Dec. 7, 2023), <https://www.hhs.gov/about/news/2023/12/07/hhs-office-for-civil-rights-settles-first-ever-phishing-cyber-attack-investigation.html>. [245] *Id.* [246] *Id.* [247] Press Release, Department of Homeland Security, *Statement from Secretary Mayorkas on President Biden's National Cybersecurity Strategy* (Mar. 2, 2023), <https://www.dhs.gov/news/2023/03/02/statement-secretary-mayorkas-president-bidens-national-cybersecurity-strategy>. [248] Press Release, Department of Homeland Security, *DHS Issues Recommendations to Harmonize Cyber Incident Reporting for Critical Infrastructure Entities* (Sept. 19, 2023), <https://www.dhs.gov/news/2023/09/19/dhs-issues-recommendations-harmonize-cyber-incident-reporting-critical>. [249] Brandon Wales, *CIRCIa at One Year: A Look Behind the Scenes*, Cybersecurity & Infrastructure Security Agency (Mar. 24, 2023), <https://www.cisa.gov/news-events/news/circia-one-year-look-behind-scenes>; see also Gibson Dunn's client alert on the Cyber Incident Reporting for Critical Infrastructure Act, <https://www.gibsondunn.com/president-biden-signs-into-law-the-cyber-incident-reporting-for-critical-infrastructure-act-expanding-cyber-reporting-obligations-for-a-wide-range-of-public-and-private-entities/>. [250] Press Release, Department of Homeland Security, *Joint Statement from 21 Countries and the Organization of American States Following the Department of Homeland Security Western Hemisphere Cyber Conference* (Sept. 28, 2023), <https://www.dhs.gov/news/2023/09/28/joint-statement-21-countries-and-organization-american-states-following-department>. [251] Press Release, Cybersecurity and Infrastructure Security Agency, *CISA and FBI Release Advisory on CLOP Ransomware Gang Exploiting MOVEit Vulnerability* (June 7, 2023), <https://www.cisa.gov/news-events/news/cisa-and-fbi-release-advisory-clOp-ransomware-gang-exploiting-moveit-vulnerability>.

GIBSON DUNN

[252] Press Release, Department of Homeland Security, *Cyber Safety Review Board Releases Report on Activities of Global Extortion-Focused Hacker Group Lapsus\$* (Aug. 10, 2023), <https://www.dhs.gov/news/2023/08/10/cyber-safety-review-board-releases-report-activities-global-extortion-focused>; Press Release, Department of Homeland Security, *Department of Homeland Security's Cyber Safety Review Board to Conduct Review on Cloud Security* (Aug. 11, 2023), <https://www.dhs.gov/news/2023/08/11/department-homeland-securitys-cyber-safety-review-board-conduct-review-cloud>. [253] Cybersecurity Advisory, Cybersecurity and Infrastructure Security Agency, *#StopRansomware: LockBit 3.0 Ransomware Affiliates Exploit CVE 2023-4966 Citrix Bleed Vulnerability* (Nov. 21, 2023), <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-325a>. [254] Press Release, Department of Homeland Security, *DHS Announces Additional \$374.9 Million in Funding to Boost State, Local Cybersecurity* (Aug. 7, 2023), <https://www.dhs.gov/news/2023/08/07/dhs-announces-additional-3749-million-funding-boost-state-local-cybersecurity>. [255] Press Release, Department of Justice, *Justice Department Announces New National Security Cyber Section Within the National Security Division* (June 20, 2023), <https://www.justice.gov/opa/pr/justice-department-announces-new-national-security-cyber-section-within-national-security>. [256] *Id.* [257] Press Release, Department of Justice, *U.S. Department of Justice Disrupts Hive Ransomware Variant* (Jan. 26, 2023), <https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant>. [258] *Id.* [259] Press Release, Department of Justice, *Justice Department Announces Court-Authorized Disruption of Snake Malware Network Controlled by Russia's Federal Security Service* (May 9, 2023), <https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-snake-malware-network-controlled>. [260] *Id.* [261] Press Release, Department of Justice, *Qakbot Malware Disrupted in International Cyber Takedown* (Aug. 29, 2023), <https://www.justice.gov/usao-cdca/pr/qakbot-malware-disrupted-international-cyber-takedown>. [262] Press Release, Department of Justice, *Justice Department Disrupts Proliferous ALPHV/Blackcat Ransomware Variant* (Dec. 19, 2023), <https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-allyblackcat-ransomware-variant>. [263] *Id.* [264] Press Release, Department of Justice, *Justice Department and Meta Platforms Inc. Reach Key Agreement as They Implement Groundbreaking Resolution to Address Discriminatory Delivery of Housing Advertisements* (Jan. 9, 2023), <https://www.justice.gov/opa/pr/justice-department-and-meta-platforms-inc-reach-key-agreement-they-implement-groundbreaking>. [265] *Id.* [266] *Id.*; Roy L. Austin, Jr., *An Update on Our Ads Fairness Efforts*, Meta (Jan. 9, 2023), <https://about.fb.com/news/2023/01/an-update-on-our-ads-fairness-efforts/>. [267] Press Release, Department of Justice, *Justice Department Files Statement of Interest in Fair Housing Act Case Alleging Unlawful Algorithm-Based Tenant Screening Practices* (Jan. 9, 2023), <https://www.justice.gov/opa/pr/justice-department-files-statement-interest-fair-housing-act-case-alleging-unlawful-algorithm>. [268] *Id.* [269] *Id.* [270] RESTRICT Act, S. 686, 118th Cong. (2023), <https://www.congress.gov/bill/118th-congress/senate-bill/686/text>. [271] Statements and Releases, White House, *Statement from National Security Advisor Jake Sullivan on the Introduction of the RESTRICT Act* (Mar. 7, 2023), <https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/07/statement-from-national-security-advisor-jake-sullivan-on-the-introduction-of-the-restrict-act/>; Press Release, Department of Commerce, *Statement from U.S. Secretary of Commerce Gina Raimondo on the Introduction of the RESTRICT Act* (Mar. 7, 2023), <https://www.commerce.gov/news/press-releases/2023/03/statement-us-secretary-commerce-gina-raimondo-introduction-restrict-act>. [272] RESTRICT Act, S. 686, 118th Cong. (2023), <https://www.congress.gov/bill/118th-congress/senate-bill/686/text>. [273] Protecting Americans' Data From Foreign Surveillance Act of 2023, S. 1974, 118th Cong. (2023), <https://www.congress.gov/bill/118th-congress/senate-bill/1974/text>. [274] *Id.* [275] *Id.* [276] *Id.* [277] *Id.* [278] Press Release, Office of Cybersecurity, Energy Security, and Emergency Response, *DOE Announces \$39 Million in Research Funding to Enhance Cybersecurity of Clean Distributed Energy Resources* (Sept. 12, 2023), <https://www.energy.gov/ceser/articles/doe-announces-39-million-research-funding-enhance-cybersecurity-clean-distributed>. [279] *Id.* [280] *Id.* [281] Alexandra Kelley, *Cyberattacks on Energy's National Labs Draw Lawmaker Scrutiny*, Nextgov/FCW (Feb. 2,

GIBSON DUNN

2023), <https://www.nextgov.com/cybersecurity/2023/02/cyberattacks-energys-national-labs-draw-lawmaker-scrutiny/382503/>. [282] Special Report, Department of Energy, *Management Challenges at the Department of Energy — Fiscal Year 2024* (Nov. 17, 2023), <https://www.energy.gov/sites/default/files/2023-11/DOE-OIG-24-05.pdf>. [283] *Id.* [284] Daniel Wilson, *Defense Dept. Proposes Long-Awaited Cybersecurity Rule*, Law360 (Dec. 22, 2023), <https://www.law360.com/cybersecurity-privacy/articles/1780256/defense-dept-proposes-long-awaited-cybersecurity-rule>. [285] *Id.* [286] *Id.* [287] Press Release, Federal Communications Commission, *Chairwoman Rosenworcel Launches Privacy and Data Protection Task Force* (June 14, 2023), <https://www.fcc.gov/document/chairwoman-rosenworcel-launches-privacy-and-data-protection-task-force>. [288] *Id.* [289] Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116-105, 133 Stat. 3274 (2019); Federal Communications Commission, *TRACED Act Implementation* (May 1, 2023), <https://www.fcc.gov/TRACEDAct>. [290] Limits on Exempted Calls Under the Telephone Consumer Protection Act of 1991, 88 Fed. Reg. 3668 (Jan. 20, 2023) (to be codified at 47 C.F.R. pt. 64). [291] *Id.* [292] Press Release, Federal Communications Commission, *Rosenworcel Launches Effort on AI's Impact on Robocalls and Robotexts* (Oct. 23, 2023), <https://docs.fcc.gov/public/attachments/DOC-397925A1.pdf>. [293] Federal Communications Commission, *FCC Launches Inquiry into AI's Impact on Robocalls and Robotexts* (Nov. 17, 2023), <https://www.fcc.gov/consumer-governmental-affairs/fcc-launches-inquiry-ais-impact-robocalls-and-robotexts>. [294] Federal Communications Commission, *Second Report and Order, Second Further Notice of Proposed Rulemaking in CG Docket Nos. 02-278 and 21-402, and Waiver Order in CG Docket No. 17-59* (Dec. 18, 2023), <https://docs.fcc.gov/public/attachments/FCC-23-107A1.pdf>. [295] *Id.* at 13–15. [296] *Id.* at 20 n.113. [297] Press Release, White House, *Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers* (July 18, 2023), <https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smart-devices-to-protect-american-consumers/>. [298] *Id.* [299] Press Release, Federal Communications Commission, *FCC Fact Sheet on Proposed Voluntary Cybersecurity Labeling Program for Internet-Enabled Devices* (Aug. 10, 2023), <https://docs.fcc.gov/public/attachments/DOC-395909A1.pdf>. [300] Press Release, Federal Communications Commission, *FCC Adopts Updated Data Breach Notification Rules To Protect Consumers* (Dec. 13, 2023), <https://docs.fcc.gov/public/attachments/DOC-399090A1.pdf>. [301] *Id.* [302] Press Release, Federal Communications Commission, *FCC Proposes \$20M Fine for Apparently Failing to Protect Consumer Data* (July 28, 2023), <https://docs.fcc.gov/public/attachments/DOC-395581A1.pdf>. [303] *Id.* [304] *A New Landmark for Consumer Control Over Their Personal Information: CPPA Proposes Regulatory Framework for Automated Decisionmaking Technology*, Cal. Privacy Protection Agency (Nov. 27, 2023), <https://cppa.ca.gov/announcements/2023/20231127.html>; see also *Draft Automated Decisionmaking Technology Regulations*, Cal. Privacy Protection Agency (Dec. 8, 2023), https://cppa.ca.gov/meetings/materials/20231208_item2_draft.pdf. [305] *CPPA to Review Privacy Practices of Connected Vehicles and Related Technologies*, Cal. Privacy Protection Agency (July 31, 2023), <https://cppa.ca.gov/announcements/2023/20230731.html>. [306] *Ahead of Privacy Day, Attorney General Bonta Focuses on Mobile Applications' Compliance with the California Consumer Privacy Act*, Cal. Att'y Gen. (Jan. 27, 2023), <https://oag.ca.gov/news/press-releases/ahead-data-privacy-day-attorney-general-bonta-focuses-mobile-applications%E2%80%99>. [307] *Attorney General Bonta Seeks Information from California Employers on Compliance with California Consumer Privacy Act*, Cal. Att'y Gen. (July 14, 2023), <https://oag.ca.gov/news/press-releases/attorney-general-bonta-seeks-information-california-employers-compliance>. [308] Complaint, *People v. Google*, Case No. 23CV422424 (Santa Clara Cnty. Super. Ct., Sept. 14, 2023), <https://oag.ca.gov/system/files/attachments/press->

GIBSON DUNN

[docs/Filed%20stamped%20Google%20Complaint.pdf](#). [309] Attorney General James Seeks information from Madison Square garden Regarding Use of Facial Recognition Technology to Deny Entry to Venues, N.Y. Att'y Gen. (Jan. 25, 2023), <https://ag.ny.gov/press-release/2023/attorney-general-james-seeks-information-madison-square-garden-regarding-use>. [310] DFS Announces \$1 million Cybersecurity Settlement with First American Title Insurance Company, N.Y. Dept. of Fin. Servs. (Nov. 28, 2023), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202311281 [311] *Id.* [312] AG Ferguson's lawsuit forces Google to pay nearly \$40M over deceptive location tracking, Wash. Att'y Gen. (May 18, 2023) <https://www.atg.wa.gov/news/news-releases/ag-ferguson-s-lawsuit-forces-google-pay-nearly-40m-over-deceptive-location>. [313] Press Release, Office of the Indiana Attorney General, Attorney General Todd Rokita Secures \$49.5 Million Multistate Settlement with Blackbaud for Data Breach (Oct. 5, 2023), https://events.in.gov/event/attorney_general_todd_rokita_secures_495_million_multistate_settlement_with_blackbaud_for_data_breach. [314] Press Release, New York State Office of the Attorney General, Attorney General James and Multistate Coalition Secure \$6.5 Million from Morgan Stanley for Failing to Protect Customer Data (Nov. 16, 2023), <https://ag.ny.gov/press-release/2023/attorney-general-james-and-multistate-coalition-secure-65-million-morgan-stanley>. [315] Press Release, New Jersey Office of the Attorney General, AG Platkin Co-Leads \$2.5-Million Multistate Settlement with EyeMed Over Data Breach that Compromised the Personal Information of Millions of Patients (May 16, 2023), <https://www.njoag.gov/ag-platkin-co-leads-2-5-million-multistate-settlement-with-eyemed-over-data-breach-that-compromised-the-personal-information-of-millions-of-patients/>. [316] See Notice of Settlement and Joint Stipulation and [Proposed] Order to Stay Litigation Activities Pending Filing of Mot. for Prelim. Approval, *In re Orrick, Herrington & Sutcliffe, LLP Data Breach Litig.*, No. 3:23-cv-04089 (N.D. Cal. Dec. 21, 2023), ECF No. 50. [317] See Order Granting Final Approval of Class Action Settlement and Pls.' Mot. for Att'ys' Fees and Costs, *Desue v. 20/20 Eye Care Network Inc.*, No. 21-61275 (S.D. Fla. July 8, 2023), ECF No. 100. [318] Identity Theft Resource Center, Q3 2023 Data Breach Analysis, https://www.idtheftcenter.org/wp-content/uploads/2023/10/20231011_Q3-2023-Data-Breach-Analysis.pdf. [319] Identity Theft Resource Center, Q3 2022 Data Breach Analysis, https://www.idtheftcenter.org/wp-content/uploads/2022/10/20221005_One-Page-Q3-2022-Data-Breach-Analysis.pdf. [320] See Transfer Order, *In re MOVEit Customer Data Sec. Breach Litig.*, MDL No. 3083 (J.P.M.L. Oct. 4, 2023); Judicial Panel on Multidistrict Litigation, *MDL Statistics Report – Distribution of Pending MDL Dockets by Actions Pending* (Jan. 2, 2014), https://www.jpml.uscourts.gov/sites/jpml/files/Pending_MDL_Dockets_By_Actions_Pending-January-2-2024.pdf. [321] See *In re MOVEit Customer Data Sec. Breach Litig.*, No. 23-3083 (D. Mass.). [322] *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021) (holding that plaintiffs who had not suffered concrete harm due to data breach, and instead claimed they are at heightened risk of future harm, lack standing to sue under Article III). [323] *Id.* at 437. [324] 72 F.4th 365, 375 (1st Cir. 2023) (holding that plaintiff adequately alleged standing based on the filing of a fraudulent tax return that likely resulted from information compromised in the data breach). [325] *Id.* at 377. [326] *Bohnak v. Marsh & McLennan Cos., Inc.*, 79 F.4th 276, 286 (2d Cir. 2023) (cleaned up). [327] *Id.* at 287. [328] 2023 WL 4183380, at *4 (E.D. Va. June 26, 2023). [329] *Id.* [330] *Id.* [331] *Id.* [332] *Id.* at *5. [333] 2023 WL 5608389, at *2 (C.D. Cal. Aug. 29, 2023) (acknowledging that while an increased risk of identity theft stemming from a data breach can constitute a threat of imminent harm sufficient for standing purposes, on the facts of the case, the username and password stolen in the breach were not linked to the plaintiff's financial accounts, and thus did not give rise to the threat of identity theft). [334] *Id.* [335] See *TransUnion*, 594 U.S. at 431 ("Every class member must have Article III standing in order to recover individual damages. Article III does not give federal courts the power to order relief to any uninjured plaintiff, class action or not."). [336] 344 F.R.D. 38, 52 (D.D.C. 2023). [337] *Id.* at 53. [338] *Id.* at 55. [339] See Cornerstone Research, *Securities Class Action Trend Cases*, <https://www.cornerstone.com/insights/research/securities-class-action-trend-cases/>. [340] Complaint ¶ 3, *Jaramillo v. Dish Networks Corp.*, No. 23-734 (D. Colo. Mar. 23, 2023), ECF No. 1. [341] Complaint ¶ 4, *Official Intel. Pty. Ltd., v. Block, Inc.*, No. 23-2789 (S.D.N.Y. April 3, 2023), ECF No. 1. [342] 15 U.S.C. § 78u-4(b)(2). [343] *In re Okta, Inc.*

GIBSON DUNN

Securities Litig., 2023 WL 2749193, at *20 (N.D. Cal. Mar. 31, 2023). [344] *Id.* at *15. [345] *Id.* [346] See, e.g., *Javier v. Assurance IQ, LLC*, 2022 WL 1744107 (9th Cir. May 31, 2022); *Popa v. Harriet Carter Gifts, Inc.*, 45 F.4th 687 (3d Cir. 2022). [347] 18 U.S.C. § 2510 *et seq.* [348] *Id.* § 2511(2)(d). [349] See Recording Law, *All Party (Two Party) Consent States – List and Details*, <https://recordinglaw.com/party-two-party-consent-states/> (last visited Jan. 26, 2024) (identifying 13 two-party or all-party consent states). [350] See, e.g., Cal. Penal Code §§ 631, 632 (wiretapping and eavesdropping statutes); *id.* § 637.2(a) (authorizing a private right of action and statutory damages). [351] *Doe v. Regents of Univ. of California*, No. 23-CV-00598-WHO, 2023 WL 3316766 (N.D. Cal. May 8, 2023). [352] *Jackson v. Fandom, Inc.*, No. 22-CV-04423-JST, 2023 WL 4670285 (N.D. Cal. July 20, 2023). [353] *Id.* at *4–5. [354] *Stark v. Patreon, Inc.*, 656 F. Supp. 3d 1018 (N.D. Cal. 2023). [355] *Id.* at 1039–40. [356] 18 U.S.C. § 1030(a). [357] *Van Buren v. United States*, 141 S. Ct. 1648, 1654–55 (2021). [358] Press Release, Department of Justice, *Department of Justice Announces New Policy for Charging Cases under the Computer Fraud and Abuse Act* (May 19, 2022), <https://www.justice.gov/opa/press-release/file/1507126/download>. [359] *United States v. Calonge*, 74 F.4th 31, 36 (2d Cir. 2023), *cert. denied*, 2023 WL 7475309 (U.S. Nov. 13, 2023). [360] *Id.* at 33–34. [361] *Id.* at 33. [362] *Id.* at 33–34. [363] *Id.* at 35–36 (citing 18 U.S.C. § 1030(e)(8)). [364] *Calonge v. United States*, 2023 WL 7475309 (U.S. Nov. 13, 2023). [365] *ACW Flex Pack LLC v. Wrobel*, 2023 WL 4762596, at *6–7 (N.D. Ill. July 26, 2023). [366] *Id.* at *3, *6. [367] *Id.* at *5. [368] *Id.* at *6. [369] *Id.* (quoting 18 U.S.C. § 1030(e)(1)) (emphasis removed). [370] *Id.* at *6–8. [371] *Id.* at *7. [372] *iPurusa, LLC v. Bank of New York Mellon Corp.*, 2023 WL 3072686, at *7 (D.N.J. Apr. 25, 2023). [373] *Id.* at *6. [374] *Id.* at *7. [375] *Id.* [376] See, e.g., *T. et al v. OpenAI LP et al.*, Case No. 23-cv-04557, Dkt. 1 ¶¶ 317–326 (N.D. Cal.); *P.M. et al v. OpenAI LP et al.*, Case No. 23-cv-03199-TLT, Dkt. 1 ¶¶ 422–431 (N.D. Cal.); see *id.* Dkt. 38 (notice of voluntary dismissal). [377] *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180 (9th Cir. 2022). [378] *Id.* at 1201. [379] Cal. Penal Code §§ 502(c)(2) & (e)(1). [380] *Id.* § 502(b)(1). [381] *Brown v. Google LLC*, 2023 WL 5029899, at *1 (N.D. Cal. Aug. 7, 2023). [382] *Id.* at *2. [383] *Id.* at *18. [384] *Id.* at *19 (citing Cal. Penal Code § 502(c)(2)). [385] *Id.* [386] *Brown et al. v. Google LLC*, Case No. 4:20-cv-03664, Dkt. 1089 (N.D. Cal.). [387] *Nora Gutierrez v. Converse Inc.*, 2023 WL 8939221, at *1, *5 (C.D. Cal. Oct. 27, 2023). [388] *Id.* at *4 (quoting *In re iPhone Application Litig.*, 2011 WL 4403963, at * 12 (N.D. Cal. Sept. 20, 2011)). [389] *Id.* [390] *Id.* at *5. [391] 47 U.S.C. § 227. [392] *Facebook, Inc. v. Duguid*, 592 U.S. 395 (2021). [393] *Dickson v. Direct Energy, LP*, 69 F.4th 338, 348–49 (6th Cir. 2023). [394] *Id.* at 345–48. [395] *Drazen v. Pinto*, 74 F.4th 1336, 1345–46 (11th Cir. 2023) (reversing *Salcedo v. Hanna*, 936 F.3d 1162, 1172 (11th Cir. 2019)). [396] *Hall v. Smosh Dot Com, Inc.*, 72 F.4th 983, 990–91 (9th Cir. 2023). [397] *Id.* at 990. [398] *Mauthe v. Millennium Health LLC*, 58 F.4th 93, 97 (3d Cir. 2023). The TCPA defines an “unsolicited advertisement” as “any material advertising the commercial availability or quality of any property, goods, or services which is transmitted to any person without that person’s prior express invitation or permission, in writing or otherwise.” 47 U.S.C. § 227(a)(5). [399] *Trim v. Reward Zone USA LLC*, 76 F.4th 1157, 1164 (9th Cir. 2023). [400] Cal. Civ. Code § 1798.150 (West 2023). [401] *California Consumer Privacy Act (CCPA) Litigation*, U.S. Cybersecurity and Data Privacy Outlook and Review - 2023 (Jan. 30, 2023), <https://www.gibsondunn.com/us-cybersecurity-and-data-privacy-outlook-and-review-2023/>. [402] Order Granting Final Approval of Class Action Settlement, *Service v. Volkswagen Grp. of Am., Inc.*, No. C22-01841 (Cal. Super. Ct. Contra Costa Cnty. May. 31, 2023), <https://odyportal.cc-courts.org/Portal/DocumentViewer/DownloadDocumentFile/Download?d=10C938A76250CE4331774F2C729A0D43&c=EC610BADE930EF833C9117C84F5729FC&l=4C398088907DD05C6D76FE93BC04CDF4&cn=F44FB09A29DC4F11FE28DCC41D39CD99&fileName=C22-01841%20-%20Order%20Filed%20Re%20Granting%20Final%20Approval&docTypeId=3&isVersionId=False>. [403] *Id.* at 4. [404] *Carter v. Vivendi Ticketing US LLC*, No. SACV2201981(DFMx), 2023 WL 8153712 (C.D. Cal. Oct. 30, 2023). [405] *Id.* [406] *Id.* at *2. [407] *Gershfeld v. Teamviewer US, Inc.*, No. SACV2100058(ADSx), 2021 WL 3046775 (C.D. Cal. June 24, 2021). [408] *Id.* at 2. [409] *Gershfeld v. TeamViewer US, Inc.*, No. 21-55753, 2023 WL 334015 (9th Cir. Jan. 20, 2023) (mem.). [410] *Alexander v. Wells Fargo Bank, N.A.*, No. 23-CV-617-DMS-BLM, 2023 WL 5109532 (S.D. Cal. Aug. 9, 2023). [411] *California Consumer Privacy Act*

GIBSON DUNN

(CCPA) Litigation, U.S. Cybersecurity and Data Privacy Outlook and Review - 2023 (Jan. 30, 2023), <https://www.gibsondunn.com/us-cybersecurity-and-data-privacy-outlook-and-review-2023/>. [412] *Brown v. Google LLC*, No. 4:20-CV-3664, 2023 WL 5029899 (N.D. Cal. Aug. 7, 2023). [413] *Id.* [414] *Id.* at *21. [415] *Id.* [416] *Id.* at *21. [417] *Id.* [418] Cal. Civ. Code § 1798.150(b). [419] *California Consumer Privacy Act (CCPA) Litigation*, U.S. Cybersecurity and Data Privacy Outlook and Review - 2023 (Jan. 30, 2023), <https://www.gibsondunn.com/us-cybersecurity-and-data-privacy-outlook-and-review-2023/>. [420] *Guy v. Convergent Outsourcing, Inc.*, No. C22-1558, 2023 WL 4637318 (W.D. Wash. July 20, 2023). [421] Cal. Civ. Code § 1798.150(b). [422] *Guy*, 2023 WL 4637318. [423] *Griffey v. Magellan Health Inc.*, No. CV-20-01282-PHX, 2022 WL 1811165, at *6 (D. Ariz. June 2, 2022). [424] *Guy*, 2023 WL 4637318, at *9. [425] *Florence v. Order Express, Inc.*, No. 22 C 7210, 2023 WL 3602248 (N.D. Ill. May 23, 2023). [426] *Id.* at *7 (internal quotations omitted). [427] Cal. Civ. Code § 1798.150(b). [428] *Florence*, 2023 WL 3602248, at *7. [429] *California Consumer Privacy Act (CCPA) Litigation*, U.S. Cybersecurity and Data Privacy Outlook and Review - 2023 (Jan. 30, 2023), <https://www.gibsondunn.com/us-cybersecurity-and-data-privacy-outlook-and-review-2023/>. [430] *Durgan v. U-Haul Int'l Inc.*, No. CV-22-01565-PHX, 2023 WL 7114622 (D. Ariz. Oct. 27, 2023). [431] *Id.* at *7. [432] *Id.* at *6. [433] *In re Bank of Am. California Unemployment Benefits Litig.*, No. 21-MD-2992-LAB-MSB, 2023 WL 3668535 (S.D. Cal. May 25, 2023). [434] *Id.* at *13–15. [435] *Id.* at *15. [436] *Tims v. Black Horse Carriers, Inc.*, 216 N.E.3d 845 (Ill. 2023). [437] 735 Ill. Comp. Stat. Ann. 5/13-205 (2022). [438] *Tims*, 216 N.E.3d at 854. [439] *Cothron v. White Castle Sys., Inc.*, 216 N.E.3d 918, 920 (Ill. 2023). [440] *Id.* at 928. [441] *Id.* at 929. [442] *Minor v. Oldcastle Servs. Inc.*, No. 21?CV?503?SMY (S.D. Ill. Mar. 22, 2023). [443] *Jones v. Microsoft Corp.*, No. 1:22?cv?03437 (N.D. Ill. Jan. 9, 2023). [444] *Id.* at 7–8. [445] *Warmack?Stillwell v. Christian Dior, Inc.*, No. 22?C?4633 (N.D. Ill. Feb. 10, 2023). [446] *Crumpton v. Octapharma Plasma, Inc.*, 513 F. Supp. 3d 1006, 1015–17 (N.D. Ill. 2021). [447] *Id.* [448] Tex. Bus. & Com. Code § 503.001. [449] *Tex. v. Meta Platforms, Inc.*, Cause No. 22-0121 (Tex. Dist. Ct. Feb. 8, 2023). [450] Press Release, Attorney General of Texas, *Paxton Sues Google for its Unauthorized Capture and Use of Biometric Data and Violation of Texans' Privacy* (Oct. 20, 2022), <https://texasattorneygeneral.gov/news/releases/paxton-sues-google-its-unauthorized-capture-and-use-biometric-data-and-violation-texans-privacy>. [451] *Gross v. Madison Square Garden Ent. Corp.*, No. 1:23-cv-03380 (S.D.N.Y. filed Apr. 21, 2023). [452] Second Amended Complaint at 2–3, *Gross v. Madison Square Garden Ent. Corp.*, No. 1:23-cv-03380 (S.D.N.Y. June 9, 2023). [453] *Id.* [454] *Id.* at 23–24. [455] *Id.* at 25. [456] Report & Recommendation, *Gross v. Madison Square Garden Ent. Corp.*, No. 23-cv-3380 (S.D.N.Y. Jan. 9, 2024). [457] *Id.* at 14. [458] *Id.* at 18. [459] *Id.* at 20 (quoting *Zoll v. Ruder Finn, Inc.*, No. 01-cv-139 (CSH), 2004 WL 42260, at *4 (S.D.N.Y. Jan. 7, 2004)). [460] *Id.* at 21. [461] *Id.* at 8–13. [462] 598 U.S. 471 (2023). [463] 598 U.S. 617 (2023). [464] *Taamneh*, 598 U.S. at 482. [465] *Gonzalez*, 598 U.S. at 621. [466] *Taamneh*, 598 U.S. at 501–02. [467] *Gonzalez*, 598 U.S. at 622. [468] *Minahan v. Google LLC*, No. 22-cv-5652, 2023 WL 3605329, at *1 (N.D. Cal. May 1, 2023), *appeal filed*, No. 23-15775 (9th Cir. May 22, 2023). [469] *Id.* at *2. [470] *M.K. v. Google LLC*, No. 21-cv-08465, 2023 WL 4937287 (N. D. Cal. filed Oct. 29, 2021). [471] *Id.* at *10. [472] *Id.* at *3. [473] *Id.* [474] *Id.* at *5. [475] *Id.* at *6–7. [476] *Ramirez v. The Paradies Shops, LLC*, 69 F.4th 1213, 1221 (11th Cir. 2023). [477] *Id.* at 1216. [478] *Id.* [479] *Id.* at 1220–21. [480] Class Action Complaint at 2–3, *Pai v. Tesla, Inc.*, Case 4:23-cv-04550 (N.D. Cal. filed Sept. 5, 2023). [481] *Id.* [482] *The Digital Revolution Engineering Smart City Infrastructure*, Utilities One (Oct. 27, 2023), <https://utilitiesone.com/the-digital-revolution-engineering-smart-city-infrastructure>. [483] Ashley Johnson, *Balancing Privacy and Innovation in Smart Cities and Communities*, Info. Tech. & Innovation Found. (Mar. 6, 2023), <https://itif.org/publications/2023/03/06/balancing-privacy-and-innovation-in-smart-cities-and-communities/>. [484] *Id.* [485] Diana Baker Freeman, *Why Local Governments Are a Target for Cyber Attacks and Steps to Prevent It*, Governing (May 6, 2022), <https://www.governing.com/sponsored/why-local-governments-are-a-target-for-cyber-attacks-and-steps-to-prevent-it>. [486] Richard Forno, *Local Governments Are Attractive Targets for Hackers and Are Ill-Prepared*, Ctr. for Internet & Soc'y (Mar. 28,

GIBSON DUNN

2022), <https://cyberlaw.stanford.edu/blog/2022/03/local-governments-are-attractive-targets-hackers-and-are-ill-prepared>. [487] Ashley Johnson, *Balancing Privacy and Innovation in Smart Cities and Communities*, Info. Tech. & Innovation Found. (Mar. 6, 2023), <https://itif.org/publications/2023/03/06/balancing-privacy-and-innovation-in-smart-cities-and-communities/>. [488] *Id.* [489] Maya Shwayder, *The Future of Smart Cities May Mean the Death of Privacy*, Digit. Trends (Apr. 22, 2020), <https://www.digitaltrends.com/news/smart-cities-privacy-security/>. [490] Ashley Johnson, *Balancing Privacy and Innovation in Smart Cities and Communities*, Info. Tech. & Innovation Found. (Mar. 6, 2023), <https://itif.org/publications/2023/03/06/balancing-privacy-and-innovation-in-smart-cities-and-communities/>. [491] *What is Edge Computing?*, IBM (last visited Jan. 18, 2024), <https://www.ibm.com/topics/edge-computing>. [492] Mary K. Pratt, *7 Edge Computing Trends to Watch in 2023 and Beyond*, TechTarget (Dec. 8, 2022), <https://www.techtarget.com/searchcio/tip/Top-edge-computing-trends-to-watch-in-2020>. [493] *Id.* [494] *Id.* [495] *Id.* [496] Pete Swabey, *Why Edge Computing is a Double-Edged Sword for Privacy*, Tech Monitor (Mar. 31, 2023), <https://techmonitor.ai/focus/privacy-on-the-edge-why-edge-computing-is-a-double-edged-sword-for-privacy>. [497] *Id.* [498] *Id.* [499] *Id.* [500] Matthew Gooding, *Can GAIA-X Solve Europe's Data Sovereignty Problem?*, Tech Monitor (Apr. 8, 2021), <https://techmonitor.ai/technology/cloud/what-is-gaia-x-eu-data-sovereignty>. [501] Executive Office of the President, Office of Science and Technology Policy, *National Strategy To Advance Privacy-Preserving Data Sharing and Analytics* (Mar. 2023), <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf>. [502] OECD, *Emerging Privacy-Enhancing Technologies, Current Regulatory and Policy Approaches*, OECD Digital Economy Papers, No. 351, 2 (Mar. 2023), <https://www.oecd-ilibrary.org/deliver/bf121be4-en.pdf?itemId=/content/paper/bf121be4-en&mimeType=pdf>. [503] Executive Office of the President, Office of Science and Technology Policy, *National Strategy To Advance Privacy-Preserving Data Sharing and Analytics* (Mar. 2023), <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf>. [504] *Id.* [505] *Id.* [506] *Id.* [507] *Id.* [508] *Id.* [509] *Id.* [510] *Id.* [511] Pete Swabey, *Why Edge Computing is a Double-Edged Sword for Privacy*, Tech Monitor (Mar. 31, 2023), <https://techmonitor.ai/focus/privacy-on-the-edge-why-edge-computing-is-a-double-edged-sword-for-privacy>. [512] Executive Office of the President, Office of Science and Technology Policy, *National Strategy To Advance Privacy-Preserving Data Sharing and Analytics* (Mar. 2023), <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf>. [513] *Id.* [514] Shafi Goldwasser et al., *The Knowledge Complexity of Interactive Proof Systems*, 18 SIAM J. Computing 186 (1989). [515] Eli Ben-Sasson et al., *Zerocash: Decentralized Anonymous Payments from Bitcoin*, Zerocash, (May 18, 2014), <http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf>. [516] Tianyi Liu et al., *zkCNN: Zero Knowledge Proofs for Convolutional Neural Network Predictions and Accuracy*, Comput. & Comm'n's Sec. (2021), <https://doi.org/10.1145/3460120.3485379>. [517] Executive Office of the President, Office of Science and Technology Policy, *National Strategy To Advance Privacy-Preserving Data Sharing and Analytics* (Mar. 2023), <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf>. [518] *Id.* [519] *Id.* [520] Jennifer Bryant, *European Commission Adopts EU-US Adequacy Decision*, Int'l Ass'n Priv. Pros. (July 10, 2023), <https://iapp.org/news/a/european-commission-adopts-eu-u-s-adequacy-decision/>. [521] *Id.* [522] Natasha Lomas, *Europe's Top Court Strikes Down Flagship EU-US Data Transfer Mechanism*, TechCrunch (July 16, 2020), <https://techcrunch.com/2020/07/16/europes-top-court-strikes-down-flagship-eu-us-data-transfer-mechanism/>. [523] Natasha Lomas, *Europe Adopts US Data Adequacy Decision*, TechCrunch (July 10, 2023), <https://techcrunch.com/2023/07/10/eu-us-data-privacy-framework-adoption/>. [524] *Id.* [525] *Id.* [526] Press Release, Department of Commerce, *Data Privacy Framework Program Launches New Website Enabling U.S. Companies to Participate in Cross-Border Data Transfers* (July 17, 2023), <https://www.commerce.gov/news/press-releases/2023/07/data-privacy-framework->

GIBSON DUNN

[program-launches-new-website-enabling-us](#). [527] Press Release, Senator Ron Wyden, *Wyden, Lee, Davidson and Lofgren Introduce Bipartisan Legislation to Reauthorize and Reform Key Surveillance Law, Secure Protections for Americans' Rights* (Nov. 7, 2023), <https://www.wyden.senate.gov/news/press-releases/wyden-lee-davidson-and-lofgren-introduce-bipartisan-legislation-to-reauthorize-and-reform-key-surveillance-law-secure-protections-for-americans-rights>. [528] Noah Chauvin & Elizabeth Goitein, *Reform Bill Would Protect Americans from Warrantless Surveillance*, Brennan Ctr. for Just. (Nov. 7, 2023), <https://www.brennancenter.org/our-work/analysis-opinion/reform-bill-would-protect-americans-warrantless-surveillance>. [529] On December 22, 2023, President Biden signed the National Defense Authorization Act, which included a Congressional measure extending Section 702 until mid-April 2024. Rebecca Beitsch, *Congress Approves Short-Term Extension of Warrantless Surveillance Powers*, *The Hill* (Dec. 12, 2023), <https://thehill.com/policy/national-security/4360341-fisa-congress-approves-short-term-extension-warrantless-surveillance-powers>; see also Press Release, White House, *Joseph R. Biden, Statement from President Biden on H.R. 2670, National Defense Authorization Act for Fiscal Year 2024* (Dec. 22, 2023), <https://www.whitehouse.gov/briefing-room/statements-releases/2023/12/22/statement-from-president-joe-biden-on-h-r-2670-national-defense-authorization-act-for-fiscal-year-2024/>. [530] Noah Chauvin & Elizabeth Goitein, *Reform Bill Would Protect Americans from Warrantless Surveillance*, Brennan Ctr. for Just., (Nov. 7, 2023), <https://www.brennancenter.org/our-work/analysis-opinion/reform-bill-would-protect-americans-warrantless-surveillance>. [531] *Id.* [532] *Id.* [533] *Id.* [534] *Id.* [535] *Electronic Communications Privacy Act (ECPA)*, Elec. Priv. Info. Ctr. (last visited Jan. 19, 2024), <https://epic.org/ecpa/>; see also Press Release, Senator Ron Wyden, *Wyden, Lee, Davidson and Lofgren Introduce Bipartisan Legislation to Reauthorize and Reform Key Surveillance Law, Secure Protections for Americans' Rights* (Nov. 7, 2023), <https://www.wyden.senate.gov/news/press-releases/wyden-lee-davidson-and-lofgren-introduce-bipartisan-legislation-to-reauthorize-and-reform-key-surveillance-law-secure-protections-for-americans-rights>. [536] *Government Surveillance Reform Act of 2023*, S. 3234, 118th Cong. (2023). [537] *Id.* § 504. [538] *Id.*; 47 U.S.C. § 230(f) (2000). [539] *Government Surveillance Reform Act of 2023*, S. 3234, 118th Cong. § 504 (2023). [540] *Id.* § 501–11. [541] *Id.* [542] *Id.* § 508. [543] *Id.* § 503. [544] India McKinney, *The House Intelligence Committee's Surveillance 'Reform' Bill is a Farce*, Elec. Frontier Found. (Dec. 8, 2023), <https://www.eff.org/deeplinks/2023/12/section-702-needs-reform-and-oversight-not-expansion-congress-should-oppose-hpsci>; see also Jules Roscoe, *Congress Pulls Bill That Would Massively Expand Surveillance After 'Dramatic Showdown'*, *Vice* (Dec. 12, 2023), <https://www.vice.com/en/article/y3wkdg/fisa-surveillance-bill-congress-pulled>. [545] Jules Roscoe, *Congress Pulls Bill That Would Massively Expand Surveillance After 'Dramatic Showdown'*, *Vice* (Dec. 12, 2023), <https://www.vice.com/en/article/y3wkdg/fisa-surveillance-bill-congress-pulled>. [546] *Id.* [547] Press Release, ACLU, *Ahead of House Vote, ACLU Sounds Alarm on Bill Greatly Expanding the Government's Mass Warrantless Surveillance Authority* (Dec. 11, 2023), <https://www.aclu.org/press-releases/ahead-of-house-vote-aclu-sounds-alarm-on-bill-greatly-expanding-the-governments-mass-warrantless-surveillance-authority>.

The following Gibson Dunn lawyers assisted in preparing this alert: Alexander Southwell, Cassandra Gaedt-Sheckter, Natalie Hausknecht, Martie Kutscher Clark, Timothy Loose, Abbey Barrera, Jacob Arber, Tony Bedel, Matt Buongiorno, Eric Hornbeck, Jay Mitchell*, Wesley Sze, Terry Wong, Najatt Ajarar, Michael Brandon, Tawkir Chowdhury, Lanie Corrigan, Justine Deitz, Skylar Drefcinski, Sasha Dudding, Kunal Kanodia, Erin Kim, Brendan Krimsky, Ruby Lang, Emma Li, Ignacio Martinez Castellanos, Jay Minga, Peter Moon, Narayan Narasimhan*, Mason Pazhwak, Matthew Reagan, John Ryan, Christopher Scott*, Becca Smith, Snezhana Stadnik Tapia, Graham Miller Stinnett, Cydney Swain, Julie Sweeney, Trenton Van Oss, Hayato Watanabe, Diego Wright, and Samantha Yi*.

Gibson Dunn lawyers are available to assist in addressing any questions you may have about these developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any leader or member of the firm's Privacy, Cybersecurity & Data Innovation practice group: **United States:** S. Ashlie Beringer – Co-Chair, Palo Alto (+1

GIBSON DUNN

650.849.5327, aberinger@gibsondunn.com) Jane C. Horvath – Co-Chair, Washington, D.C. (+1 202.955.8505, jhorvath@gibsondunn.com) Ryan T. Bergsieker – Denver (+1 303.298.5774, rbergsieker@gibsondunn.com) Gustav W. Eyler – Washington, D.C. (+1 202.955.8610, geyler@gibsondunn.com) Cassandra L. Gaedt-Sheckter – Palo Alto (+1 650.849.5203, cgaedt-sheckter@gibsondunn.com) Svetlana S. Gans – Washington, D.C. (+1 202.955.8657, sgans@gibsondunn.com) Lauren R. Goldman – New York (+1 212.351.2375, lgoldman@gibsondunn.com) Stephenie Gosnell Handler – Washington, D.C. (+1 202.955.8510, shandler@gibsondunn.com) Natalie J. Hausknecht – Denver (+1 303.298.5783, nhausknecht@gibsondunn.com) Martie Kutscher Clark – Palo Alto (+1 650.849.5348, mkutscherclark@gibsondunn.com) Kristin A. Linsley – San Francisco (+1 415.393.8395, klinsley@gibsondunn.com) Timothy W. Loose – Los Angeles (+1 213.229.7746, tloose@gibsondunn.com) Vivek Mohan – Palo Alto (+1 650.849.5345, vmohan@gibsondunn.com) Rosemarie T. Ring – San Francisco (+1 415.393.8247, rring@gibsondunn.com) Ashley Rogers – Dallas (+1 214.698.3316, arogers@gibsondunn.com) Alexander H. Southwell – New York (+1 212.351.3981, asouthwell@gibsondunn.com) Eric D. Vandevelde – Los Angeles (+1 213.229.7186, evandevelde@gibsondunn.com) Benjamin B. Wagner – Palo Alto (+1 650.849.5395, bwagner@gibsondunn.com) Debra Wong Yang – Los Angeles (+1 213.229.7472, dwongyang@gibsondunn.com) **Europe:** Ahmed Baladi – Co-Chair, Paris (+33 (0) 1 56 43 13 00, abaladi@gibsondunn.com) Nicholas Banasevic* – Managing Director, Brussels (+32 2 554 72 40, banasevic@gibsondunn.com) Kai Gesing – Munich (+49 89 189 33-180, kgesing@gibsondunn.com) Joel Harrison – London (+44 20 7071 4289, jharrison@gibsondunn.com) Vera Lukic – Paris (+33 (0) 1 56 43 13 00, vlukic@gibsondunn.com) Lars Petersen – Frankfurt/Riyadh (+49 69 247 411 525, lpetersen@gibsondunn.com) Robert Spano – London/Paris (+44 20 7071 4000, rspano@gibsondunn.com) **Asia:** Connell O'Neill – Hong Kong (+852 2214 3812, coneill@gibsondunn.com) Jai S. Pathak – Singapore (+65 6507 3683, jpathak@gibsondunn.com) **Nicholas Banasevic, Managing Director in the firm's Brussels office and an economist by background, is not admitted to practice law. *Jay Mitchell and Samantha Yi are associates in the Washington, D.C. office. Jay is admitted in California and Illinois, and Samantha is admitted in Maryland; both are practicing under supervision of members of the District of Columbia Bar under D.C. App. R. 49. *Narayan Narasimhan and Christopher Scott, recent law graduates in the New York office, are not admitted to practice law.* © 2024 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. Attorney Advertising: These materials were prepared for general informational purposes only based on information available at the time of publication and are not intended as, do not constitute, and should not be relied upon as, legal advice or a legal opinion on any specific facts or circumstances. Gibson Dunn (and its affiliates, attorneys, and employees) shall not have any liability in connection with any use of these materials. The sharing of these materials does not establish an attorney-client relationship with the recipient and should not be relied upon as an alternative for advice from qualified counsel. Please note that facts and circumstances may vary, and prior results do not guarantee a similar outcome.

Related Capabilities

[Privacy, Cybersecurity, and Data Innovation](#)

GIBSON DUNN



Securities Enforcement Update

July 25, 2024

Dismissal of Much of SEC's SolarWinds Complaint Has Potentially Broad Implications for SEC Cybersecurity Enforcement

The SEC's action against SolarWinds related to a highly publicized compromise of the company in 2020 that was attributed to Russia's Foreign Intelligence Service who had inserted malware into a routine SolarWinds software update.

On July 18, 2024, the U.S. District Court for the Southern District of New York largely granted SolarWinds' motion to dismiss and dismissed most of the SEC's claims against the company and its former Chief Information Security Officer (CISO).^[1] The SEC's action against SolarWinds related to a highly publicized compromise of the company in 2020 that was attributed to Russia's Foreign Intelligence Service (SVR) who had inserted malware into a routine SolarWinds software update. Although thousands of SolarWinds customers received the software update, the SVR used the compromise to access the environments of certain SolarWinds customers in the government and private sector (the "SUNBURST" incident).

The court dismissed most of the claims advanced by the SEC relating to its disclosures, including SolarWinds' Form 8-K filings, but did sustain claims against SolarWinds and its CISO alleging that a "Security Statement" posted on its website in 2017 may have been false or misleading.

The decision is noteworthy for several reasons:

- The court dismissed the SEC's claim that cybersecurity-related deficiencies were actionable under its rules relating to internal accounting and disclosure controls. The

court concluded that the claim was “ill-pled” because “cybersecurity controls are not—and could not have been expected to be—part of the apparatus necessary to the production of accurate” financial reports, noting that “[a]s a matter of statutory construction, [the SEC’s] reading is not tenable.”^[2] This is noteworthy because the SEC just last month entered into a settlement in cybersecurity-related case under the theory that internal accounting controls-related regulations could encompass traditional IT assets that were unrelated to financial systems or financial/accounting data.^[3] The Solar Winds decision will likely impact how the SEC thinks about its broad use of accounting controls as a basis to charge a violation related to a cyber incident.

- The court’s decision makes clear that more than isolated disclosure failures are required to put the adequacy of a company’s disclosure controls and procedures in issue. The decision also leaves open the question of whether, in a close case where the SEC may be inclined to allege fraud, the SEC will continue to be willing to enter into a settlement on the basis of a disclosure controls and procedures violation if the company was willing to do so in order to avoid a fraud charge, as has been their practice to date.
- While the decision is an encouraging sign that the SEC’s aggressive attempts to hold CISOs individually liable for company conduct will be evaluated on the factual record and the law, the decision did not dismiss all claims against the CISO (allowing the claims based on allegations of contemporaneous knowledge of falsity of public statements to go forward), and companies and CISOs should remain vigilant in responding to cybersecurity incidents and ensuring the accuracy of all public statements that are made about cybersecurity.

Background

On October 30, 2023, the SEC filed a complaint against SolarWinds and its former CISO alleging that they made materially false and misleading statements and omissions on the company website, blog posts, press releases, Form S-1, and quarterly and annual SEC reports *prior* to the incident and did the same in two reports on Form 8-K in which the company disclosed the incident.^[4] The SEC also conducted an investigation regarding the SUNBURST incident and issued a letter to certain companies because the SEC staff believed those entities were impacted by the SolarWinds compromise and requested that they provide information to the staff on a voluntary basis.^[5] In February 2024, the SEC filed an amended complaint including factual details to support its allegations that SolarWinds and its CISO were aware of the company’s weak security practices yet made contrary statements about its strength in SolarWinds’ Security Statement.^[6] The Defendants filed a motion to dismiss in March 22, 2024,^[7] and the court issued its order on July 18, 2024.

July 18, 2024 Order

The court largely granted Defendants’ motion to dismiss, sustaining only the SEC’s claims alleging securities fraud based on allegations that the company made false or misleading representations in a “Security Statement” posted to SolarWinds’ website. Specifically:

1. Fraud and False and Misleading Statements

The court dismissed most of the SEC’s securities fraud claims regarding SolarWinds’ statements about its strong security that it made in press releases, blog posts, podcasts and securities

filings. However, the court allowed the SEC's claims based on the Securities Statement on SolarWinds' website to proceed.[\[8\]](#)

The "Security Statement"

The court found that the SEC adequately pled that the Security Statement posted on SolarWinds' website contained materially misleading and false representations as to at least two of SolarWinds' cybersecurity practices: access controls and password protection policies. The court's holding was based on the allegations in the complaint that SolarWinds had made statements touting that it had strong access controls and password policies when its internal practices and discourse instead "portrayed a diametrically opposite representation for public consumption."[\[9\]](#) Specifically, the court found that the complaint alleged that the company's access controls had "deficiencies" that "were not only glaring—they were long-standing, well-recognized within the company, and unrectified over time," and its password policies were generally not enforced.[\[10\]](#) The court also found that the amended complaint "amply" alleged scienter, including that the former CISO knew of the substantial body of data that impeached the security statement's content as false and misleading.[\[11\]](#)

The court importantly explained that false statements on public websites can sustain securities fraud liability, as the security statement at issue appeared on SolarWinds' public website, accessible to all, including investors, and therefore was, according to the court, unavoidably part of the "total mix of information" that SolarWinds furnished to the investing public.[\[12\]](#) The court emphasized that for purposes of evaluating materiality, each representation should be considered collectively, rather than in isolation, as investors evaluate the whole picture.

Press Releases, Blog Posts, and Podcasts

The court dismissed the SEC's claims that SolarWinds made false and misleading statements related to the 2020 incident in press releases, blog posts, and podcasts explaining that each qualifies as non-actionable corporate puffery, "too general to cause a reasonable investor to rely upon them."[\[13\]](#) As the court noted, while public statements, such as the website security statement, can serve as the basis for a material misstatement when they contain a degree of specificity, general statements by an issuer about the strength of their cybersecurity program were not sufficient to support a fraud violation.

Pre-Incident Public Filings

The court dismissed each of the SEC's claims that SolarWinds' cybersecurity risk disclosures in its SEC filings did not accurately reflect the risks that the company faced. The court found that, viewed in totality, the risk disclosures sufficiently alerted the investing public of the types and nature of the cybersecurity risks SolarWinds faced and the consequences these could present for the company's financial health and future.[\[14\]](#) The court also held that, on the facts pled, SolarWinds was not required to amend its cybersecurity risk disclosures for certain cyber incidents as the company's cybersecurity risk disclosures already warned investors of the risks "in sobering terms."[\[15\]](#)

In the court's view, issuers are not required to disclose cybersecurity risks with "maximum specificity," as, according to the court, spelling out a cybersecurity risk may backfire in various ways, such as by arming malevolent actors with information to exploit or by misleading investors as other disclosures might be disclosed with relatively less specificity.^[16]

Post-incident Form 8-K

The court found that the SEC did not adequately plead that the post-incident Form 8-K was materially false or misleading, as the disclosure fairly captured the known facts and disclosed what was required for reasonable investors. The court also acknowledged that the impact on stock prices indicated that the market "got the message" (noting SolarWinds' share prices dropped more than 16% the day of the announcement, and another 8% the next day),^[17] and emphasized that SolarWinds published the disclosure just two days after discovering the compromise, when it was still in the early phases of its investigation and had a limited understanding of the attack.

2. Internal Accounting Controls

The court found that the SEC's attempt to bring a claim under Section 13(b)(2)(B) of the Exchange Act (relating to internal accounting controls) was unsupported by legislative intent, as the surrounding terms that Congress used when drafting Section 13(b)(2)(B), which refer to "transactions," "preparation of financial statements," "generally accepted accounting principles," and "books and records," are uniformly consistent with financial accounting.^[18] The court's deep skepticism of the claim that Congress intended to confer the SEC with such authority is reflected in the analogy that doing so would be tantamount to "hid[ing] elephants in mouseholes."^[19] The court also found that the few courts that interpreted the term "internal accounting controls" as used in this section "have consistently construed it to address financial accounting."^[20] In this respect, the court's conclusion is consistent with the views expressed in several dissents by Commissioners in other settled enforcement actions in which the SEC has used the internal accounting controls provision to impose liability for non-financial related conduct.^[21]

3. Disclosure Controls and Procedures

The court sided with SolarWinds in rejecting the SEC's claims that the company failed to maintain and adhere to appropriate disclosure controls for cybersecurity incidents. The court was unwilling to accept the SEC's argument that one-off issues—even if the company misapplied its existing disclosure controls in considering cybersecurity incidents—gave rise to a claim that the company failed to maintain such controls. Importantly, this case relates to conduct prior to the adoption of the SEC's 2023 cybersecurity rules, which have made it even more important for companies to maintain appropriate controls.

The court acknowledged that SolarWinds had misclassified the severity level of two incidents under its Incident Response Plan (IRP) and failed to elevate a vulnerability to the CEO and CTO for disclosure.^[22] However, the court found that these instances—without more—did not support a claim that SolarWinds maintained ineffective disclosure controls.

The SEC did not plead deficiency in the “construction” of SolarWinds’ IRP, nor did it allege routine misclassification of incidents or frequent errors as a result of applying that framework.^[23] The court implied that disclosure controls do not have to be perfect—they should provide *reasonable assurance* that information is being collected for disclosure consideration. The court thus found that the one-off issues identified by the SEC in applying the IRP and associated cybersecurity disclosure controls were not, without more, sufficient to “plausibly impugn [a] company’s disclosure controls systems.”^[24]

Key Takeaways

Internal Accounting Controls.

- Notably, on June 18, 2024 the SEC claimed in a settlement that another company that had experienced cyber incidents violated rules relevant to internal accounting controls. The SEC alleged that the company failed to “provide reasonable assurances...that access to company assets is permitted only in accordance with management’s...authorization.”^[25] The SEC’s claims and approach in that settlement were seen as particularly aggressive as the predicate cybersecurity incident (for which the controls would be relevant) did not impact financial systems or corporate financial and accounting data. That settlement also evoked a notable dissent from two Commissioners arguing that the internal accounting controls provision did not apply to a company’s overall cybersecurity program.
- The court in this case comprehensively repudiated the SEC’s effort to bring an internal accounting controls violation based on Section 13(b)(2)(B) in the context of cybersecurity-related actions. The court found the SEC’s position that their authority to regulate an issuer’s “system of internal accounting controls” includes authority to regulate cybersecurity controls “not tenable,” and unsupported by the statute, legislative intent, or precedent. ^[26] The court held that the statute cannot be construed to broadly cover all systems public companies use to safeguard their valuable assets and that the statute’s reach is limited as it governs systems of “internal *accounting* controls.”^[27]
- As such, the SolarWinds decision calls into question—and may signal an end to—the SEC’s recent attempts to adopt an expansive reading of its rules relating to internal accounting controls to govern cybersecurity controls—whether or not such cybersecurity controls are relevant to the production of financial reports.

Disclosure Controls and Procedures.

- The decision also calls into question the SEC’s ability to rely on claims of inadequate disclosure controls and procedures in similar circumstances, given that the court found that more than a single disclosure failure is required to put the adequacy of a company’s disclosure controls and procedures in issue.
- While this fact-based finding provides reassurance that good-faith, day-to-day mistakes at a company may not be actionable, it remains important to design and maintain disclosure controls that provide for appropriate escalation and consideration.

Assessing Fraud Claims Based on Public Disclosures.

- When evaluating the accuracy of public disclosures in the context of a securities fraud claim, representations are to be evaluated based on a holistic assessment, rather than each statement in isolation. The court rearticulated the long-standing view the investing public “evaluates the information available to it ‘as a whole.’” Nevertheless, a securities fraud claim may be pursued where there is evidence that the company—or a CISO or other company officer—is aware of inaccuracies at the time such statements are made.

[1] Opinion and Order, *SEC v. SolarWinds Corp. and T. Brown*, 1:23-cv-09518-PAE (S.D.N.Y. July 18, 2024) (hereinafter “Order”).

[2] Order at 3, 94–102.

[3] See Gibson Dunn Client Alert, “SEC as Cybersecurity Regulator” (June 20, 2024), available at <https://www.gibsondunn.com/wp-content/uploads/2024/06/sec-as-cybersecurity-regulator.pdf?v2>; R.R. Donnelley & Sons, No. 3-21969 (S.E.C. June 18, 2024) (order instituting cease and desist proceedings), available at <https://www.sec.gov/files/litigation/admin/2024/34-100365.pdf>.

[4] Complaint, *SEC v. SolarWinds Corp. and T. Brown*, No. 23-cv-9518 (Oct. 30, 2023), <https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-227.pdf>.

[5] In the Matter of Certain Cybersecurity-Related Events (HO-14225) FAQs, U.S. Securities and Exchange Commission, available at <https://www.sec.gov/enforce/certain-cybersecurity-related-events-faqs>.

[6] Am. Compl., *SEC v. SolarWinds Corp. and T. Brown*, No. 23-cv-9518-PAE (S.D.N.Y. Feb. 20, 2024).

[7] Mem. of Law in Support of Mot. to Dismiss, *SEC v. SolarWinds Corp. and T. Brown*, No. 23-cv-9518-PAE (S.D.N.Y. Mar. 22, 2024).

[8] See Order at 3.

[9] Order at 54.

[10] Order at 54.

[11] Order at 61.

[12] Order at 51 (citation omitted).

[13] Order at 68 (citation omitted).

[14] Order at 71–79.

[15] Order at 75.

[16] Order at 73.

[17] Order at 90.

[18] Order at 96.

[19] Order at 100.

[20] Order at 97–98.

[21] [2023 Year-End Securities Enforcement Update - Gibson Dunn](#) (end notes 20–22); SEC Statement, The SEC’s Swiss Army Statute: Statement on Charter Communications, Inc. (Nov. 14, 2023), available at https://www.sec.gov/news/statement/peirce-uyeda-statement-charter-communications-111423#_ftn6.

[22] Order at 102–106.

[23] Order at 104.

[24] Order at 106.

[25] R.R. Donnelley & Sons, No. 3-21969 (S.E.C. June 18, 2024) (order instituting cease and desist proceedings), available at <https://www.sec.gov/files/litigation/admin/2024/34-100365.pdf>.

[26] Order at 96.

[27] Order at 96–97.

The following Gibson Dunn lawyers prepared this update: Mark Schonfeld, David Woodcock, Ronald Mueller, Brian Lane, Vivek Mohan, Stephenie Gosnell Handler, Sophie Rohnke, Michael Roberts, Sarah Pongrace, and Ashley Marcus.

Gibson Dunn lawyers are available to assist in addressing any questions you may have regarding these developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any leader or member of the firm’s [Securities Enforcement](#), [Privacy, Cybersecurity & Data Innovation](#), or [Securities Regulation & Corporate Governance](#) practice groups:

Securities Enforcement:

[Tina Samanta](#) – New York (+1 212.351.2469, tsamanta@gibsondunn.com)

Mark K. Schonfeld – New York (+1 212.351.2433, mschonfeld@gibsondunn.com)
David Woodcock – Dallas/Washington, D.C. (+1 214.698.3211, dwoodcock@gibsondunn.com)

Privacy, Cybersecurity and Data Innovation:

Ahmed Baladi – Paris (+33 (0) 1 56 43 13 00, abaladi@gibsondunn.com)
S. Ashlie Beringer – Palo Alto (+1 650.849.5327, aberinger@gibsondunn.com)
Stephenie Gosnell Handler – Washington, D.C. (+1 202.955.8510, shandler@gibsondunn.com)
Joel Harrison – London (+44 20 7071 4289, jharrison@gibsondunn.com)
Jane C. Horvath – Washington, D.C. (+1 202.955.8505, jhorvath@gibsondunn.com)
Vivek Mohan – Palo Alto (+1 650.849.5345, vmohan@gibsondunn.com)
Rosemarie T. Ring – San Francisco (+1 415.393.8247, rring@gibsondunn.com)
Sophie C. Rohnke – Dallas (+1 214.698.3344, srohnke@gibsondunn.com)

Securities Regulation and Corporate Governance:

Elizabeth Ising – Washington, D.C. (+1 202.955.8287, eising@gibsondunn.com)
Thomas J. Kim – Washington, D.C. (+1 202.887.3550, tkim@gibsondunn.com)
Brian J. Lane – Washington, D.C. (+1 202.887.3646, blane@gibsondunn.com)
Julia Lapitskaya – New York (+1 212.351.2354, jlapitskaya@gibsondunn.com)
James J. Moloney – Orange County (+1 1149.451.4343, jmoloney@gibsondunn.com)
Ronald O. Mueller – Washington, D.C. (+1 202.955.8671, rmueller@gibsondunn.com)
Michael Scanlon – Washington, D.C. (+1 202.887.3668, mscanlon@gibsondunn.com)
Lori Zyskowski – New York (+1 212.351.2309, lzyskowski@gibsondunn.com)

Attorney Advertising: These materials were prepared for general informational purposes only based on information available at the time of publication and are not intended as, do not constitute, and should not be relied upon as, legal advice or a legal opinion on any specific facts or circumstances. Gibson Dunn (and its affiliates, attorneys, and employees) shall not have any liability in connection with any use of these materials. The sharing of these materials does not establish an attorney-client relationship with the recipient and should not be relied upon as an alternative for advice from qualified counsel. Please note that facts and circumstances may vary, and prior results do not guarantee a similar outcome.

If you would prefer NOT to receive future emailings such as this from the firm,
please reply to this email with "Unsubscribe" in the subject line.

If you would prefer to be removed from ALL of our email lists,
please reply to this email with "Unsubscribe All" in the subject line. Thank you.

© 2024 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at gibsondunn.com

GIBSON DUNN



Securities Regulation & Corporate Governance
Update

December 12, 2024

Cybersecurity Disclosure Overview: A Survey of Form 10-K Cybersecurity Disclosures by S&P 100 Companies

This update discusses key trends and insights from our analysis of the cybersecurity disclosures made by 97 S&P 100 companies in their most recent Form 10-K filings in response to Regulation S-K Item 106.

I. Introduction

This alert highlights key trends and insights from our analysis of the cybersecurity disclosures made by 97 S&P 100 companies in their 2024 Form 10-K filings, as required by new Item 106 of Regulation S-K (“Item 106”), as of November 30, 2024.^[1]

As discussed in a previous [client alert](#), the Securities and Exchange Commission (“SEC” or “Commission”) adopted on July 26, 2023, a final rule requiring public companies to provide current disclosure of material cybersecurity incidents and annual disclosure regarding cybersecurity risk management, strategy, and governance. Under Item 106, which is required to be addressed in new Item 1C of Form 10-K, public companies must include disclosures in their annual reports regarding their (1) cybersecurity risk management and strategy, including with respect to their processes for identifying, assessing, and managing cybersecurity threats and whether risks from cybersecurity threats have materially affected them, and (2) cybersecurity governance, including with respect to oversight by their boards and management.^[2] All public companies were required to comply with these disclosure requirements for the first time

beginning with their annual reports on Form 10-K or 20-F for the fiscal year ending on or after December 15, 2023.

II. Executive Overview

While certain disclosure trends have emerged under Item 106, we note that there is significant variation among companies' cybersecurity disclosures, reflecting the reality that effective cybersecurity programs must be tailored to each company's specific circumstances, such as its size and complexity of operations, the nature and scope of its activities, industry, regulatory requirements, the sensitivity of data maintained, and risk profile. Companies must strike a careful balance in their disclosures, providing sufficient decision-useful information for investors, while taking care not to reveal sensitive information that could be exploited by threat actors.^[3] We expect company disclosures to continue to evolve as their practices change in response to the ever-evolving cybersecurity threat landscape and as common disclosure practices emerge among public companies.

Below is an executive overview of the key disclosure trends we observed (discussed in detail in Section III below):

- **Materiality.** The phrasing used by companies for this disclosure requirement varies widely. Specifically, in response to the requirement to describe whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect the company, the largest group of companies (40%) include disclosure in Item 1C largely tracking Item 106(b)(2) language (at times, subject to various qualifiers); 38% vary their disclosure from the Item 106(b)(2) requirement in how they address the forward-looking risks; and 22% of companies do not include disclosure specifically responsive to Item 106(b)(2) directly in Item 1C, although a substantial majority of these companies cross-reference to a discussion in Item 1A "Risk Factors."
- **Board Oversight.** Most companies delegate specific responsibility for cybersecurity risk oversight to a board committee and describe the process by which such committee is informed about such risks. Ultimately, however, the majority of surveyed companies report that the full board is responsible for enterprise-wide risk oversight, which includes cybersecurity.
- **Cybersecurity Program.** Companies commonly reference their program alignment with one or more external frameworks or standards, with the National Institute of Standards and Technology (NIST) Cybersecurity Framework being cited most often. Companies also frequently discuss specific administrative and technical components of their cybersecurity programs, as well as their high-level approach to responding to cybersecurity incidents.
- **Assessors, Consultants, Auditors or Other Third Parties.** As required by Item 106(b)(1)(ii), nearly all companies discuss retention of assessors, consultants, auditors or other third parties, as part of their processes for oversight, identification, and management of material risks from cybersecurity threats.
- **Risks Associated with Third-Party Service Providers and Vendors.** In line with the requirements of Item 106(b)(1)(iii), all companies outline processes for overseeing risks associated with third-party service providers and vendors.
- **Drafting Considerations.**

- Most companies organize their disclosure into two sections, generally tracking the organization of Item 106, with one section dedicated to cybersecurity risk management and strategy and another section focused on cybersecurity governance. Companies typically include disclosures responsive to the requirement to address material impacts of cybersecurity risks, threats, and incidents in the section on risk management and strategy.
- The average length of disclosure among surveyed companies is 980 words, with the shortest disclosure at 368 words and the longest disclosure at 2,023 words. The average disclosure runs about a page and a half.

While comment letters have not been issued in response to Item 106 disclosure in annual reports on Form 10-K filed by the S&P 100 companies we surveyed, as of November 30, 2024, five comment letters from the Staff had been issued to other companies regarding their Item 106 disclosures. For details, see Section VI below.

III. Key Disclosure Trends

For comparison purposes, we have grouped the discussion below into three categories: (1) cybersecurity risk management and strategy; (2) cybersecurity governance; and (3) disclosures in response to the requirement to address material cybersecurity risks, threats, and incidents.

a. Cybersecurity Risk Management and Strategy

Item 106(b)(1) calls for a description of a company's "processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes." In response to this overarching disclosure requirement, some of the most commonly addressed topics are as follows:

- **Cybersecurity Frameworks or Standards.** Though not specifically required by Item 106, a majority of surveyed companies (60%) reference one or more external frameworks or standards that inform, to varying degrees, their cybersecurity program management processes and practices. The NIST Cybersecurity Framework is referenced most often, with 51 companies making mention of it. Other frameworks or standards cited by surveyed companies include those set by the International Organization for Standardization (ISO) (including, for example, ISO 27001 and 27002), SOC 1 and 2, and the Payment Card Industry Data Security Standard (PCI DSS). Notably, companies use varied terminology when discussing specified frameworks or standards. For example, when citing NIST, companies explain that their cybersecurity program or risk management approach "leveraged," was "informed by," "aligns with," or was "based on" the framework.^[4]
- **Description of Cybersecurity Program Elements.** Nearly all surveyed companies discuss specific components of the company's cybersecurity program, which most prominently include references to identity and access management, logging and monitoring, penetration testing and vulnerability scanning, governance, risk assessment and threat intelligence, employee awareness and training, and security monitoring. Companies also widely note where employees are provided with cybersecurity training (84%), with 27 of those companies disclosing that they provide this training on at least an annual basis.

- **Incident Response Preparedness.** The substantial majority of companies note the implementation of an incident response plan or procedures (87%), and nearly all companies (96%) describe the use of audits, drills, and/or tabletop exercises to test incident preparedness and the company's incident response processes.

In addition to the general requirement quoted above, Item 106(b)(1) includes a non-exclusive list of disclosure items, which most surveyed companies specifically address in their Item 1C disclosures as follows:

- **Whether and how any such processes have been integrated into the company's overall risk management system or processes.** In response to this disclosure item, a substantial majority of surveyed companies (90%) disclose that the oversight of cybersecurity risk has been integrated into the company's overall risk management system or processes.
- **Whether the registrant engages assessors, consultants, auditors or other third parties in connection with any such processes.** Nearly all companies (98%) generally disclose the engagement of assessors, consultants, auditors or other third parties in the management of cybersecurity risks. Most companies do not specifically name the third parties they engage.
- **Whether the registrant has processes to oversee and identify material risks from cybersecurity threats associated with its use of any third-party service provider.** In line with Item 106's requirements, all companies generally discuss third-party risk management practices, including outlining processes for identifying and managing material cyber risks associated with third-party service providers. Ninety percent report evaluating, monitoring or conducting due diligence on a vendor's cybersecurity practices, and 42% report requiring vendors to adhere to certain cybersecurity management processes. These third-party risk management processes can range from conducting due diligence of the third party's information security environments, or reviewing their incident response capabilities, to monitoring their regulatory compliance to assess the company's own risk of exposure.

b. Cybersecurity Governance

Item 106(c)(1) requires that companies describe the role of the board in the oversight of cybersecurity risks, including the role of board committees or subcommittees, and Item 106(c)(2)(i) requires that companies describe the management's role in assessing and managing their material risks from cybersecurity threats, including addressing which management positions or committees are responsible for assessing and managing such risks. In response to these disclosure requirements, some of the most commonly addressed topics are as follows:

- **The Role of the Board and Committees of the Board in Cybersecurity Governance.** As part of the discussion of cybersecurity governance, a majority of surveyed companies (68%) report that the board is responsible for enterprise-wide risk oversight, which includes cybersecurity. However, a majority of companies (66%) also disclose that a committee or subcommittee of the board has been delegated responsibility for primary oversight of cybersecurity risks, with a minority of companies (28%) reporting that the board and a designated committee share the primary oversight of cybersecurity risks, and

a handful of companies (6%) reporting that the full board retains primary oversight of cybersecurity risks. Of the companies that delegate primary oversight of cybersecurity risks to a committee or subcommittee, or for which the board and a designated committee or subcommittee share oversight, companies most often disclose that the audit committee (78%) has this responsibility, followed by a risk committee (19%) (for companies that have a risk committee).

- **The Role of Management in Cybersecurity Governance.** In responding to this disclosure item, nearly all companies (99%) list one or more management positions responsible for addressing and managing cybersecurity risks, with a significant minority of companies (43%) reporting that a management committee is also responsible for managing such risks. Of the companies that identify a management position responsible for assessing and managing material cybersecurity risks, 61% identify one officer who fulfills this role and 39% identify more than one officer responsible for fulfilling this role. The substantial majority of companies (78%) identify a Chief Information Security Officer (CISO) among the management positions responsible for assessing and managing cybersecurity risks, while a minority of companies identify other positions, such as a Chief Information Officer (CIO) (14%), Chief Technology Officer (CTO) (4%), or another officer, such as a Chief Security Officer, Head of Technology, Chief Information and Digital Officer, and/or Chief Cybersecurity Officer.

Item 106(c)(2)(i) also requires a description of the relevant expertise of management in “such detail as necessary to fully describe the nature of the expertise.” In response, a substantial majority of companies (88%) disclose the experience and/or qualifications of the individual(s) responsible for assessing and managing cybersecurity risk. While companies vary widely with respect to the level of specificity they provide in describing relevant experience or qualifications of those in management, surveyed companies generally provide examples of an individual’s:

- **Roles and Positions Prior to Joining the Company.** Practice on this point varies widely, ranging from the inclusion of a general note stating that the individual has held various cybersecurity-related roles, to identifying the specific title held by such individual in the past roles, to noting the technical and industry-specific experience gained or skills employed in prior positions.
- **Years of Relevant Work Experience.** Where surveyed companies disclose this point, the years of experience range from 15 years to more than 30 years of relevant work experience.
- **Education and Certifications.** While less common than the other two categories mentioned above, some companies include reference to an individual’s educational background or certifications (e.g., where the individual received certification as an information systems security professional (CISSP)).

Item 106(c)(2)(ii) requires that companies address how management is informed of and monitors the “prevention, detection, mitigation, and remediation of cybersecurity incidents.” In response to this disclosure item, companies generally disclose that management is informed of cybersecurity risks and incidents through internal reporting channels, such as receiving reports from the company’s cybersecurity professionals.

Item 106(c)(2)(iii) requires that companies discuss the process by which management reports cybersecurity risks to its board. In response to this disclosure item, all companies disclose that the board or responsible committee receives reports from management, with a substantial

majority of these companies (82%) disclosing that the board or responsible committee receives reports on a regular basis.^[5] A majority of the surveyed companies (61%) also report a process for escalating certain cybersecurity incidents, risks or threats to the board or responsible committee.

c. Material Cybersecurity Risks, Threats & Incidents

Item 106(b)(2) requires that companies “[d]escribe whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant, including its business strategy, results of operations, or financial condition and if so, how.” While disclosure on this point varied greatly, we observed the following trends among surveyed companies in response to this disclosure item:

- **Some Companies Did Not Affirmatively Address Item 106(b)(2) in Item 1C.** Twenty-two percent of surveyed companies do not appear to have included disclosure responsive to Item 106(b)(2) in Item 1C.^[6] Of these companies, 90% provide a cross-reference to a discussion in Item 1A “Risk Factors.”^[7]
- **Most Disclosures Track the Language of Item 106(b)(2).** Forty percent of surveyed companies largely track the language of the disclosure item with respect to both the backward-looking aspect (“have materially affected”) and the forward-looking aspect (“are reasonably likely to materially affect”) of the rule by responding in the negative, concluding that they did not identify any risks from cybersecurity threats that have materially affected or are reasonably likely to materially affect the company, including its business strategy, result of operations or financial condition. However, the precise formulation varied from company to company.^[8] Of these companies:
 - 54% include a knowledge qualifier making clear that they are “not aware” or “do not believe” that such risks have materially affected or are reasonably likely to materially affect the company;
 - 67% make clear that they are speaking as of the end of the fiscal year covered by the Form 10-K or as of the date of the Form 10-K;
 - in addition to tracking the rule, 44% include a disclaimer noting that there is no “guarantee” or “assurance” (or something similar) that cyber-related risks may not be material in the future;
 - 26% limit required disclosure to threats identified during the last year or last three fiscal years; and
 - one company limited the future horizon to “over the long term.”
- **Many Companies Vary Disclosure on Forward-Looking Impacts, or Address It Vaguely or Not At All.** Thirty-eight percent of surveyed companies address the backwards-looking aspect of the rule by largely tracking the rule on that point. For the forward-looking aspect of the rule, some of them: (i) simply do not address it at all or make vague references to potential future impacts (35%); (ii) include a disclaimer noting that there is no “guarantee” or “assurance” (or something similar) that cyber-related risks may not be material in the future (51%); or (iii) make explicit what is an inherent assumption in the disclosure requirement, such as by stating that risks from cybersecurity threats, “if realized,” are reasonably likely to materially affect business strategy, results of operations, or financial condition (16%). One company includes both a “no guarantee”

disclaimer and “if realized” language (3%). In addition, among these 38% of the surveyed companies:

- 16% include a knowledge qualifier making clear that they are “not aware” or “do not believe” that such risks have materially affected the company;
- 41% make clear that they are speaking as of the end of the fiscal year covered by the Form 10-K or as of the date of the Form 10-K; and
- 27% limit required disclosure to threats identified during the last year, last three fiscal years or “recent years.”

IV. ISS Governance QualityScore^[9]

While it is not possible to say definitively, it is possible that some of the reporting trends observed among the surveyed companies may be attributable to the questions included by Institutional Shareholder Services (“ISS”) in its Governance QualityScore (“QualityScore”) relating to information security since they are not otherwise directly responsive to Item 106 requirements. For example:

- possibly in response to **ISS Question 409**, which evaluates disclosure regarding whether the company has information security risk insurance, a minority of surveyed companies (26%) disclose maintaining some level of cybersecurity insurance;
- possibly in response to **ISS Question 405**, which assesses disclosure as to how many directors have information security skills, a minority of companies (14%) report having directors with information security experience, despite the fact that the proposed requirement to disclose this information was not included in the final cybersecurity rule;^[10] and
- possibly in response to **ISS Question 407**, which assesses whether a company experienced an information security breach in the last three years, 3% of companies frame their statements about material effects from cybersecurity threats or incident using this specific time period.

V. Drafting Considerations

The majority of surveyed companies (66%) divide their disclosure into two sections tracking the organization of Item 106, with one section dedicated to cybersecurity risk management and strategy and another section focused on cybersecurity governance. Of those companies, 33% include subsections within one or both of those two main sections, 23% of surveyed companies use no headings at all, and 11% of surveyed companies use headings that differ from the structure of Item 106 (either by including more than the two primary sections set forth in the rule or by including distinct headings altogether).

The average length of disclosure among surveyed companies is 980 words, with the shortest disclosure at 368 words and the longest disclosure at 2,023 words. The average disclosure runs about a page and a half.

VI. Comment Letters

As of November 30, 2024, there have been five comment letters from the Staff regarding disclosure under Item 1C. While these comment letters have not been issued in response to disclosure in annual reports on Form 10-K filed by the S&P 100 companies we surveyed, we are including a discussion of them here for completeness, as they are instructive as to what the Staff was focused on when reviewing the first set of Item 106 disclosures. To summarize:

- Two of these comment letters simply requested that companies refile their annual reports on Form 10-K to include an omitted Item 1C.[\[11\]](#) In both instances, the companies filed an amendment on Form 10-K/A, adding the requested disclosure.[\[12\]](#)
- One comment letter requested that a company amend future filings to clarify inconsistent statements about its engagement of third parties in connection with its processes for identifying, assessing and managing material risks from cybersecurity threats.[\[13\]](#) The company responded by clarifying the nature of its engagement of third parties in identifying and managing cybersecurity risks, and also confirmed that it would clarify this point to avoid any inconsistency or ambiguity in future filings.[\[14\]](#)
- In three comment letters, the Staff touched upon the following requirements of Item 106, requesting expanded disclosure in future filings:
 - **Item 106(b)(1) (*Processes for Assessing, Identifying, and Managing Material Risk from Cybersecurity Threats*)**. The Staff requested that a company expand its disclosure to describe the areas of responsibility of its executive management team and board of directors, along with their respective processes in response to this disclosure item.[\[15\]](#) The company responded by confirming it would include the requested detail in future filings.[\[16\]](#)
 - **Item 106(b)(1)(i) (*Integration of Cybersecurity Risk Processes into Overall Risk Management*)**. In one comment letter, the Staff requested that a company revise future filings to disclose how processes for “assessing, identifying, and managing” material cybersecurity threats have been integrated into its overall risk management system or processes in response to this disclosure item.[\[17\]](#) The company responded by emphasizing that these processes are “well integrated” into its overall risk management system, noting relevant disclosure included in its current filing, and agreeing to provide more detail in future filings in response to this disclosure item.[\[18\]](#)
 - **Item 106(c)(2)(i) (*Identification of Management Committees or Positions Responsible for Assessing and Managing Material Risks from Cybersecurity Threats*)**. Two of the comment letters noted above also included comments related to the discussion of management’s responsibility over cybersecurity risks. The first comment letter requested the company identify which management positions or teams are responsible for assessing and managing material risks from cybersecurity threats in future filings.[\[19\]](#) The second such letter requested a discussion of the relevant expertise of the company’s senior leadership responsible for managing the company’s cybersecurity risk and the “design and implementation of policies, processes and procedures to identify and mitigate this risk.”[\[20\]](#) In each case, the company responded by confirming it would include the requested detail in future filings.[\[21\]](#)

While the impact of the November 2024 election on future leadership of the SEC is uncertain, as are their strategic and enforcement priorities, we expect SEC scrutiny over cybersecurity incident disclosures to continue as companies adjust their disclosure practices to the new requirements.

VII. XBRL Requirements

As a reminder for the upcoming Form 10-K season, all Item 106 disclosures must be tagged in Inline XBRL (block text tagging for narrative disclosures and detail tagging for quantitative amounts) beginning one year after the initial compliance date of December 15, 2023, which, for most companies, means starting with their Form 10-K or Form 20-F filed in 2025.

Companies must use the “Cybersecurity Disclosure (CYD)” taxonomy tags within iXBRL to tag these disclosures.^[22] We note that significant judgment will be required to apply these tags. Not only will companies be required to determine the provision of Item 106 to which each part of the narrative disclosure is responsive, but companies will need to determine which flags to mark as “true” or “false.” Importantly, there is a flag for “Cybersecurity Risk Materially Affected or Reasonably Likely to Materially Affect Registrant [Flag]” and, it is our understanding that to properly apply the flag, each company must select “true” or “false.” Companies that have addressed Item 106(b)(2) by including slightly vague or ambiguous disclosure in Item 1C or by cross-referencing their risk factors will need to carefully consider how they will handle these new tagging requirements.

^[1] This alert memo highlights certain disclosure trends based on our review of the 97 surveyed companies. (As of November 30, 2024, three S&P 100 companies had not yet filed annual reports on Form 10-K for fiscal years ending on or after December 15, 2023.) Where appropriate, we have grouped together similar responses to disclosure items to enable a comparison among the companies’ disclosures. For example, where a company provided time qualifiers such as “in the last year,” “in 2023,” or “during the last fiscal year,” we have considered these to be similar data points in our survey of company disclosures. Percentages may not add up to 100% due to rounding.

^[2] Foreign private issuers are required to make similar annual disclosures pursuant to Item 16K of Form 20-F.

^[3] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11216 (July 26, 2023) (“Adopting Release”) at 60-63.

^[4] Companies are wise to be cautious when describing their adherence to cybersecurity frameworks and standards, as underscored by the SEC’s recent enforcement action against SolarWinds Corporation where the SEC charged the company with making a materially misleading statement when it claimed “SolarWinds follows the NIST Cybersecurity Framework” despite internal assessments showing that most NIST controls were not met. See *SEC v. SolarWinds Corp.*, 1:23-CV-09518 (S.D.N.Y. July 18, 2024), at 11-14.

^[5] In counting the companies who disclose where management reports to the board or responsible committee on a regular basis, we have included companies that state that they do this “regularly” (e.g., regularly, “at each regularly scheduled meeting,” etc.), as well as companies

who refer to a specific time period (e.g., annually, quarterly, semi-annually, mid-year, etc.). This does not include where companies use language such as “periodically,” “as appropriate,” “as necessary,” or “as needed.”

[6] Our review of company cybersecurity disclosure was limited to the language included in Item 1C. We have not reviewed other sections of Forms 10-K filed by surveyed companies to determine whether they contain disclosure that can be deemed responsive to Item 106(b)(2).

[7] We have not reviewed the cross-referenced risk factor, or the risk factors section more generally, to determine whether they contain disclosure that can be deemed responsive to Item 106(b)(2).

[8] The language surveyed companies use to disclose how they have been impacted by cybersecurity risks, threat, or incidents is imprecise. For example, some companies specifically discuss the effect of cybersecurity incidents, while others fully track the language of the rule and discuss “risks from cybersecurity threats”.

[9] On October 28, 2024, ISS announced an update to its ISS QualityScore product to include 12 new factors. Among these are the following Audit and Risk Oversight factors related to cybersecurity risk management:

- **Question 460.** Does the company disclose the role of the management in overseeing information security risks?
- **Question 461.** Does the company disclose the role of the board in overseeing information security risks?
- **Question 462.** Does the company have a third-party information security risk management program?
- **Question 463.** Does the company leverage a third-party assessment of information security risks?
- **Question 464.** What is the Data Protection Officer reporting line?

These factors generally align with the disclosure requirements under the rule, and based on our survey results, companies are already addressing Questions 460-463 while preparing their Item 106 disclosures.

[10] Adopting Release, *supra* note 3, at 81-85.

[11] See SEC Comment Letter to Quarta-Rad, Inc. dated August 1, 2024; SEC Comment Letter to Scientific Industries, Inc. dated June 14, 2024.

[12] See Response Letter from Quarta-Rad, Inc. to the SEC dated August 15, 2024; Response Letter from Scientific Industries, Inc. to the SEC dated July 17, 2024.

[13] See SEC Comment Letter to Wilhelmina International, Inc. dated August 21, 2024 (“SEC Letter to Wilhelmina International”).

[14] See Response Letter from Wilhelmina International, Inc. to the SEC dated September 3, 2024 (“Wilhelmina International Response Letter”).

[15] See SEC Comment Letter to TNF Pharmaceuticals, Inc. dated September 23, 2024 (“SEC Letter to TNF Pharmaceuticals”). In its comment letter, the Staff noted that the responsive disclosure needed to be in sufficient detail for a reasonable investor to understand.

[16] See Response Letter from TNF Pharmaceuticals, Inc. to the SEC dated September 30, 2024 (“TNF Pharmaceuticals Response Letter”).

[17] See SEC Comment Letter to Blackbaud, Inc. dated August 23, 2024.

[18] See Response Letter from Blackbaud, Inc. to the SEC dated September 3, 2024.

[19] SEC Letter to TNF Pharmaceuticals, *supra* note 15.

[20] SEC Letter to Wilhelmina International, *supra* note 13.

[21] Wilhelmina International Response Letter, *supra* note 14; TNF Pharmaceuticals Response Letter, *supra* note 16.

[22] See the Cybersecurity Disclosure Taxonomy Guide (September 16, 2024), available at <https://www.sec.gov/data-research/standard-taxonomies/operating-companies>.

Please click below to view the complete update and endnotes on Gibson Dunn's website:

[Read More](#)

The following Gibson Dunn lawyers assisted in preparing this update: Thomas Kim, Julia Lapitskaya, Michael Titera, Stephenie Gosnell Handler, Alexandria Johnson, Isaac Maycock, and Kayla Jahangiri.

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

Securities Regulation & Corporate Governance:

Elizabeth Ising – Co-Chair, Washington, D.C. (+1 202.955.8287, eising@gibsondunn.com)
James J. Moloney – Co-Chair, Orange County (+1 949.451.4343, jmoloney@gibsondunn.com)
Lori Zyskowski – Co-Chair, New York (+1 212.351.2309, lzyskowski@gibsondunn.com)
Aaron Briggs – San Francisco (+1 415.393.8297, abriggs@gibsondunn.com)
Thomas J. Kim – Washington, D.C. (+1 202.887.3550, tkim@gibsondunn.com)
Brian J. Lane – Washington, D.C. (+1 202.887.3646, blane@gibsondunn.com)
Julia Lapitskaya – New York (+1 212.351.2354, jlapitskaya@gibsondunn.com)
Ronald O. Mueller – Washington, D.C. (+1 202.955.8671, rmueller@gibsondunn.com)
Michael Scanlon – Washington, D.C. (+1 202.887.3668, mscanlon@gibsondunn.com)
Michael A. Titera – Orange County (+1 949.451.4365, mtitera@gibsondunn.com)

Privacy, Cybersecurity & Data Innovation:

Ahmed Baladi – Co-Chair, Paris (+33 1 56 43 13 00, abaladi@gibsondunn.com)
S. Ashlie Beringer – Co-Chair, Palo Alto (+1 650.849.5327, aberinger@gibsondunn.com)
Joel Harrison – Co-Chair, London (+44 20 7071 4289, jharrison@gibsondunn.com)
Jane C. Horvath – Co-Chair, Washington, D.C. (+1 202.955.8505, jhorvath@gibsondunn.com)
Rosemarie T. Ring – Co-Chair, San Francisco (+1 415.393.8247, rring@gibsondunn.com)
Stephenie Gosnell Handler – Washington, D.C. (+1 202.955.8510, shandler@gibsondunn.com)
Vivek Mohan – Palo Alto (+1 650.849.5345, vmohan@gibsondunn.com)
Sophie C. Rohnke – Dallas (+1 214.698.3344, srohnke@gibsondunn.com)

Attorney Advertising: These materials were prepared for general informational purposes only based on information available at the time of publication and are not intended as, do not constitute, and should not be relied upon as, legal advice or a legal opinion on any specific facts or circumstances. Gibson Dunn (and its affiliates, attorneys, and employees) shall not have any liability in connection with any use of these materials. The sharing of these materials does not establish an attorney-client relationship with the recipient and should not be relied upon as an alternative for advice from qualified counsel. Please note that facts and circumstances may vary, and prior results do not guarantee a similar outcome.

If you would prefer NOT to receive future emailings such as this from the firm,
please reply to this email with "Unsubscribe" in the subject line.

If you would prefer to be removed from ALL of our email lists,
please reply to this email with "Unsubscribe All" in the subject line. Thank you.

© 2024 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit our [website](#).