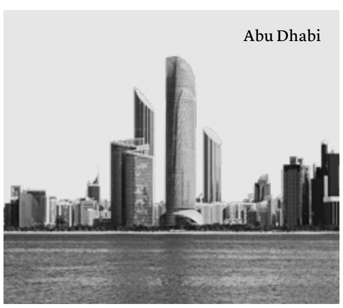
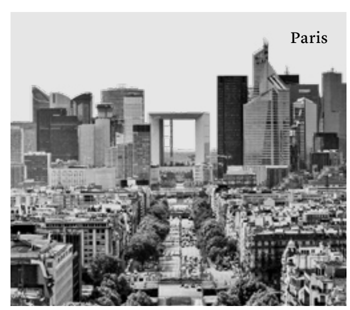
CLEARY GOTTLIEB

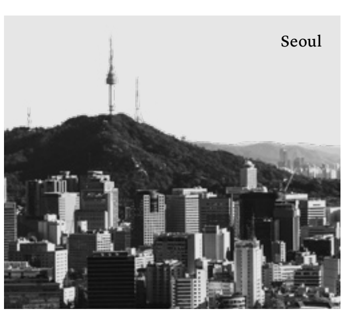
Selected Issues for Boards of Directors in 2024

January 2024

CLEARY GOTTLIEB







Selected Issues for Boards of Directors in 2024

As 2024 gets off to a busy start, companies, boards and management teams are facing a host of new and developing business issues and a large array of regulatory developments, from new and growing risks and opportunities from the adoption of artificial intelligence, to ever-changing ESG issues and backlash, as well as enhanced focus on government enforcement and review. As has become a tradition, we have asked our colleagues from around our firm to boil down those issues in their fields that boards of directors and senior management of public companies will be facing in the coming year, yielding focused updates in eighteen topics that will surely feature at the top of board agendas throughout the year.

New technologies and practices driven by AI have created fundamental business risks and opportunities that will define how businesses function in the coming decades. At the same time, the concerns and practices of public companies are evolving rapidly, driven in part by economic and societal forces accelerating the discussions and regulation around sustainability and diversity, equity and inclusion, among other factors. Companies face new disclosure requirements around cybersecurity and executive compensation at the same time as they are navigating the changing expectations on the part of politicians, regulators, institutional investors and other stakeholders. With the shifting landscape, companies are revisiting their thinking on everything from business fundamentals and how to manage liabilities and risk to corporate governance and an evolving understanding of board and management duties.

We explore these evolutions from several different angles with respect to AI, ESG, transaction activity and shareholder and activist engagements. Other topics stem from the agendas of regulators. 2023 was a notable year for developments in US tax, antitrust, sanctions, cybersecurity and privacy, labor and enforcement agency agendas. As we gear up for an election year in the United States, Congress remains mired in political skirmishes, and we expect the fast pace of regulatory rulemaking from 2023 to continue in the early part of 2024. European regulatory developments are continuing to drive board agendas as well, in areas like tax, competition and sustainability. In all of these areas, enforcement risk is on the rise and board oversight and thoughtful considerations of board structure are more critical than ever.

We invite you to review these topics by clicking on the headings listed below.

EDITORS

Francesca L. Odell

Helena K. Grannis

Jonathan Povilonis

Jake Baynum

The editors would like to thank Alejandra Alfaro-Carcoba for her invaluable contributions and appreciate her time and dedication in putting together this year's memo.

Table of Contents

AI May Do Wonders for Your Business, But What About Your Risk Profile?

David Lopez
Partner
New York
dlopez@cgsh.com

Adam Fleisher
Partner
New York
afleisher@cgsh.com

Daniel Ilan
Partner
New York
dilan@cgsh.com

Benet J. O'Reilly
Partner
Bay Area
boreilly@cgsh.com

James R. Burns
Partner
Washington, D.C.
jrburns@cgsh.com

Hugh C. Conroy, Jr.
Partner
New York
hconroy@cgsh.com

Lina Bensman
Partner
New York
lbensman@cgsh.com

Synne D. Chapman
Associate
New York
schapman@cgsh.com

Marcus Holtzman
Associate
New York
mholtzman@cgsh.com

Artificial intelligence (AI)[1] was the biggest technology news of 2023. AI continues to revolutionize business in big and small ways, ranging from disrupting entire business models to making basic support functions

[1] In referring to AI, this article is focused on the recent developments in generative AI and large language models.

more efficient. Observers have rightly focused on the plentiful value-creation opportunities this new technology affords. Less attention has been given to the risks AI creates for boards and management teams, which call for sophisticated governance, operational and risk perspectives. This article identifies key areas of risk and offers suggestions for mitigation on the road to realizing the enormous benefits AI promises.

Delays in formalized risk management and senior leadership involvement highlight the extent to which investment outpaces risk mitigation and corporate oversight strategies.

In the last year, advances in generative AI have catalyzed board level discussion of use cases and increased budgets to fund investment and adoption,[2] but for many corporations risk management lags behind and survey data indicate sub-optimal numbers of senior leaders taking ownership of AI risk management.[3] Delays in formalized risk management and senior leadership involvement highlight the extent to which investment outpaces risk mitigation and corporate oversight strategies.

Deepfakes and Public Relations

2024 will see the release of new AI tools giving average users the ability to make fake video content that is indistinguishable to the naked eye from the real thing.[4] While some commentators have considered the impact of cheap, numerous and convincing deepfakes on politics, corporations are also potential targets of smear campaigns using deepfakes to mislead – whether by way of embarrassing corporate leaders, discrediting corporate policies or manipulating stock prices through plausible, but inaccurate, videos.

Corporations and public companies, in particular, should conduct table-top exercises or otherwise develop response plans for identifying false content, proving it is not genuine and disseminating a prompt, corrective counter-narrative – all before a deepfake goes viral. Skilled advisors will be needed to navigate these nightmare scenarios, including the increasing use of third-party experts who can credibly distinguish authentic video from AI-generated fakes. Given the obvious public relations implications, it will be important to have a plan to address potential exposure, correct the record, and prepare company leaders for any necessary public statements.

Securing these services ahead of time will be a worthwhile investment if a concerted campaign is launched against a corporation or its leadership team.

Governance and the Expertise Gap

Boards can be liable to shareholders under Delaware law for a failure to adequately oversee corporate activity, including key risks. Ideally, as AI use cases are evaluated by management teams, under board oversight, both rewards and risks associated with oversight and response strategies should be analyzed. Boards should be thorough in documenting their consideration and oversight of these opportunities and the corresponding risks – while latitude is given to

2 According to the latest annual McKinsey Global Survey, 28% of respondents reporting AI adoption at their organizations have generative AI use on their board's agenda and a third of all respondents are using generative AI regularly in at least one business function. *See* McKinsey & Company "The State of AI in 2023: Generative AI's breakout year" (August 1, 2023), available here. Additionally, AI investment took center stage in budget reviews. 47% of technology officers across a variety of industries said that AI is their number one budget item over the next year, more than double the second-biggest, which is cloud-computing, according to the CNBC Technology Executive Council bi-annual survey from June 2023. *See* CNBC "A.I. is now the biggest spend for nearly 50% of top tech executives across the economy: CNBC survey" (June 23, 2023), available here.

3 KPMG surveyed 225 U.S. executives across industries in organizations with $1 billion or more in revenue in March 2023 on their views of generative AI with an updated survey of the same population in June 2023. 66% of respondents do not have a formalized AI risk management function, and do not expect to have one for periods ranging between one and four years. Although 44% of C-suite executives responded that they were directly involved in establishing new AI processes, only 33% were responsible for developing and/or implementing governance to mitigate AI risk and only 23% were responsible for review of AI risks themselves. *See* KMPG "Responsible AI and the challenge of AI risk" (2023) available here.

4 Axios "Behind the Curtain: What AI architects fear most (in 2024)" (November 8, 2023), available here.

Crisis Management

Nefarious AI use by bad actors can create a crisis at a moment's notice, making a sophisticated crisis response plan all the more imperative to successful public relations.

Holistic crisis management frameworks should be adopted and should address the three phrases of a crisis:

— **Pre-Crisis Phase (Prevention and Preparation)**

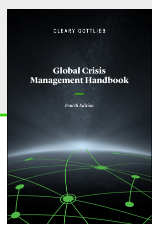
- Establish key processes in the event of a crisis and incident reporting trainings for employees.
- Identify the trusted advisors who will be prepared to give immediate support and counsel in the event that an urgent need arises.

— **During-the-Crisis Phase (Responding to the Crisis)**

- Focus on key processes surrounding comprehensive internal investigation of the crisis, public and internal communications with relevant stakeholders, monitoring of stakeholder feedback on crisis response efforts, and defense mechanisms to protect against reputational harm, economic harm, and legal liability.

— **Post-Crisis Phase (Learning from the Crisis)**

- Establish a post-crisis recovery plan, which should evaluate the handling of the crisis and lessons learned, update the crisis response plan, follow up on information requests from relevant stakeholders, identify root causes, and consider whether the incident and its root causes require further investigation and/or external consultation to resolve the root causes and/or mitigate liability and (where possible) future vulnerability or exposure.



For further discussion on crisis response and preparedness, *see* **Cleary Gottlieb Global Crisis Management Handbook: Fourth Edition**.

companies exercising business judgment in good faith, it can be more challenging to defend decision-making when the paper record does not reflect all of the care taken by the leadership. A board's satisfaction of its oversight obligation under Delaware law could come into question when AI adoption is not met with robust risk mitigation, for example, if employees leverage AI without formalized use policies in place.

Only some board and management teams, particularly outside of the tech sector, currently have meaningful in-house AI expertise or infrastructure.[5] Given the power of AI, employee use can easily become mis-use without well-developed policies and procedures. Additional recruiting and staffing may be needed, though specific requirements for use policies and senior-level AI expertise, whether in the boardroom or in the C-suite, likely will vary with how important AI is to the

[5] In a KPMG study, 53% of respondents cited a lack of appropriately skilled resources as the leading factor limiting their ability to review AI-related risks. *See* KPMG "Responsible AI and the challenge of AI risk" (2023) available here. In McKinsey's survey, just 21% of adopters said their organizations have established policies governing employees' use of AI. *See* McKinsey & Company "The State of AI in 2023: Generative AI's breakout year" (August 1, 2023), available here. At present, 68% of executives surveyed by Deloitte reported a moderate-to-extreme AI skills gap. *See* Deloitte Center for Technology, Media & Telecommunications "Talent and workforce effects in the age of AI: Insights from Deloitte's State of AI in the Enterprise, 2nd Edition survey" available here.

central business mission and how deeply embedded it is likely to become.

AI Decision-Making: Bias and Error

AI use in decision-making creates omnipresent risks across a business. For example, AI use in hiring processes could lead to claims of discrimination or bias. The idea of "AI bias" is perhaps counter-intuitive, but research has shown bias can stem from the training data, data inputs or the algorithm itself, and can exist despite the diligent efforts of developers due to subconscious cognitive biases.[6] An AI-integrated human resources function therefore can be subject to both regulatory and civil litigation risk. This is not to say that the promise of AI should be avoided in HR functions. Rather, it should be adopted with disciplined risk mitigation in focus at the outset.

Similarly, the mere allegation of faulty operational AI use in decision-making creates additional public image risk. For example, in November 2023, UnitedHealth was subject to a lawsuit claiming that its use of AI in evaluating elderly patients' qualifications for medical coverage led to a high number of errant recommendations. Regardless of the merits of the suit, the application of AI to a commonplace customer-facing business process risks public scrutiny and doubt.

Beyond public image risk, bias and error can result in significant legal and enforcement risk, particularly for highly regulated industries that are subject to consumer protection laws. For example, while noting the benefits and efficiencies of well-managed AI tools, both the Federal Reserve[7] and the Consumer Financial Protection Bureau[8] have recently warned banks and lenders about potential bias in AI that could lead to violations of fair lending, fair housing and equal opportunity laws. Similarly, the SEC has proposed substantive rules related to the use of (and potential conflicts of interest) associated with using predictive data analytics in connection with products and services offered by investment advisers and broker-dealers.[9] Other retail industries may be similarly affected, and boards in these industries should be especially cognizant of training, testing, data management and monitoring.

Regulatory

Regulation of AI is in its infancy and likely to evolve dramatically in the coming years. On October 30, 2023, the Biden Administration issued a landmark Executive Order nearly one year after publication of the Biden Administration's AI Bill of Rights. The Executive Order directs a number of federal departments and agencies to establish new standards for AI safety and security and lays the foundation for protecting various rights.[10] SEC Chairman Gary Gensler did not mince words in a recent interview with the Financial Times when he called a financial crisis within the next decade "nearly unavoidable" without "swift intervention" to regulate AI.[11] Local level regulation also is likely to expand, as illustrated by New York City's recent law requiring independent bias audits for employers using AI in hiring processes, designed to combat the exact scenario described above.[12]

6 IBM "Shedding light on AI bias with real world examples" (October 16, 2023), available here.

7 *See, e.g.,* Michael S. Barr, Vice Chair for Supervision, Board of Governors of the Federal Reserve System, *Furthering the Vision of the Fair Housing Act*, Speech at "Fair Housing at 55—Advancing a Blueprint for Equity", National Fair Housing Alliance 2023 National Conference, Washington, D.C. (July 18, 2023), available here.

8 *See, e.g.,* CFPB "CFPB Issues Guidance on Credit Denials by Lenders Using Artificial Intelligence" (September 19, 2023), available here.

9 *See* SEC Press Release "SEC Proposes New Requirements to Address Risks to Investors From Conflicts of Interest Associated With the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers" (July 26, 2023), available here.

10 For further discussion of the Biden Executive Order, *see* our November alert memo available here.

11 Financial Times "Gary Gensler urges regulators to tame AI risks to financial stability" (October 15, 2023), available here.

12 *See* NYC Local law 144 FAQs, available here.

AI is a new and very powerful tool in a cybercriminal's toolbox. Corporate leaders should prioritize cybersecurity investment and develop, or outsource AI defense mechanisms to protect their systems.

Cybersecurity

Regardless of a company's particular interest in AI adoption, contemporary cybersecurity best practices will have to evolve and adapt. For example, voice approvals for wire transfers lose their efficacy when AI can convincingly simulate voices and be used to hold conversations or appear on video conferences. AI-enabled hacking also may require more sophisticated cryptography to keep passwords, IP and other sensitive data secure. AI is a new and very powerful tool in a cybercriminal's toolbox. Corporate leaders should prioritize cybersecurity investment and develop, or outsource AI defense mechanisms to protect their systems.

Data Analytics

The efficiencies that AI adoption promises also create a risk of over-reliance that could be irreversible if the integration is not measured and strategic.

— **Knowledge Gap** – AI-related workforce reductions or innovations associated with AI could create a situation where few employees know how a particular process works.

— **Misinformation Reliance** – AI may generate or glean facts that result in patently false outputs known as "hallucinations," as exemplified by several recent high-profile instances of AI from major developers making incorrect claims during public demonstrations. AI-generated data with errors as a result of hallucinations could pollute otherwise accurate data without being noticed. This risk may compound over time as AI-generated data is used to train other AIs.

— **Decision-Making** – Reliance on generative AI without understanding its limitations could result in faulty decisions that would not be made under normal circumstances.

— **Third-Party Reliance** – Corporations that are not developing AI capabilities wholly in-house are subject to the risks posed by relying on a third-party provider. Leaders should be cautious in the event the relationship sours.

To counteract AI reliance risk, corporations should maintain highly skilled workers who mitigate knowledge gaps and monitor for statistical flaws. Highly skilled employees should be central to AI integration. AI should be a partner to subject-matter experts and data analysts, not a replacement.

M&A

The AI revolution will shift the M&A calculus for corporate leaders. The due diligence process is the traditional tool for surfacing operational and financial risks. But what happens when a target is in the AI business or has integrated AI into its business? How were the AI tools trained? Were appropriate permissions secured? Is the company dependent on certain AI tools in way that presents risk following the transaction? Is AI being used ethically and responsibly?

Sophisticated expertized diligence is required to fully understand the particularized risks an acquisition of an AI-integrated business poses to the acquirer. AI-related transactional expertise will be needed across various disciplines, such as regulatory, intellectual property, consumer protection, antitrust and privacy. As AI adoption progresses, corporate leaders should think of AI risk early and often during the M&A process and engage advisors with the requisite expertise to adequately examine the risks.

Boards of financial institutions should ensure that management is providing information about the institution's efforts for both employing AI in everyday business and controlling its risks.

Regulated Financial Services

In the financial services industry, AI offers significant promise over a wide range of financial functions from payment processing and transaction speed to fraud detection and regulatory compliance monitoring. At the same time, gaps or weaknesses in addressing and managing risks can have calamitous results for individual institutions and, through contagion, for the financial system generally.

The U.S. Financial Stability Oversight Council (FSOC) – a committee comprised of the Treasury, SEC, CFTC, Federal Reserve, OCC, FDIC, CFPB, NCUA, FHA and members from state banking and insurance agencies – recently identified use of AI for the first time as a potential vulnerability to the financial system if not monitored and managed appropriately.[13] FSOC urged its member regulators and their regulated institutions to:

— Develop design testing and controls for AI;

— Monitor the quality and applicability of both data input to, and information output from, AI;

— Apply existing regulations and guidance about financial institution use of technology to AI, while developing new policies and controls for use of AI;

— Build expertise and capacity; and

— Monitor AI innovation and development, as well as emerging risks.

[13] FSOC "Annual Report 2023" (December 14, 2023), available here.

Boards of financial institutions should ensure that management is providing information about the institution's efforts for both employing AI in everyday business and controlling its risks. External advisory resources and internal dedicated resources can enhance the board's understanding of the benefits and risks of AI. Furthermore, regulators are likely to inquire about, and examine controls for, the use of AI.[14] Therefore, boards and management should ensure they have undertaken appropriate enterprise-wide diligence and adopted policies, and coherent and consistent internal and external messages, regarding AI's use.

Key Takeaways

— AI is rich in promise but should be adopted with risk mitigation in mind to maximize value and minimize unforeseen liability.

— Senior leaders should be involved in AI adoption, and boards should be involved in its oversight, as it poses key risks in addition to great benefits.

— AI should not replace subject matter experts, but instead should be integrated with their roles to protect against over-reliance risks.

— Corporations that are not adopting AI still face risks associated with the AI revolution and should prioritize mitigating this new type of risk in all its various aspects.

[14] *See, e.g.*, Christopher J. Waller, Governor, Board of Governors of the Federal Reserve System, "Innovation and the Future of Finance" Speech at Cryptocurrency and the Future of Global Finance, Sarasota, Florida (April 20, 2023), available here; OCC, Federal Reserve, FDIC, CFPB, NCUA, "Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning" 86 Fed. Reg. 16837 (March 31, 2021), available here.

How Boards Should Be Thinking about the Supreme Court's SFFA Affirmative Action Decision

Francesca L. Odell
Partner
New York
flodell@cgsh.com

Jennifer Kennedy Park
Partner
Bay Area/New York
jkpark@cgsh.com

Charity E. Lee
Counsel
New York
charitylee@cgsh.com

In June 2023, the U.S. Supreme Court held that Harvard University and the University of North Carolina's admissions programs, which considered candidates' race in admission decisions, violated the Fourteenth Amendment of the U.S. Constitution and Title VI of the Civil Rights Act of 1964.[1] While these decisions, known collectively as *SFFA*, do not apply to a corporation's employment decisions, language in the Court's opinion has led many to speculate as to how the precedent could potentially be expanded to this context. The Court's majority noted that the language of Title VII of the Civil Rights Act, which, broadly speaking, bars discrimination in employment decisions, is almost identical to corresponding language in Title VI. Notably, in writing a concurrence joined by Justice Thomas, Justice Gorsuch observed that Title VII is "[j]ust next door" to Title VI, and noted that the majority opinion tracks the Supreme Court's prior rulings interpreting "materially identical language in Title VII," prompting Justice Gorsuch to ask rhetorically whether it makes sense to "read the same words in neighboring provisions of the same statute—enacted at the same time by the same Congress—to mean different things?"

Even before *SFFA*, so-called "reverse discrimination" claims were being pursued by employees, shareholders and watch-dog groups alleging discriminatory treatment against white, cisgendered male employees based on the defendant companies' Diversity, Equity and Inclusion (DEI) initiatives[2] Very soon after the Supreme Court issued *SFFA*, litigations challenging certain aspects of various corporate DEI programs were filed, asking courts to extend the *SFFA* majority's ruling to hold these aspects are also unconstitutional.

1 600 U.S. 181 (2023).

2 *See, e.g., Nat'l Ctr. for Pub. Policy Rsrch. v. Schultz et al.*, No. 2:22-cv-00267 (E.D. Wash. 2022) (Starbucks); *Craig v. Target Corp. et al.*, No. 2:23-cv-00599 (M.D. Fla. 2023) (Target); *Am. All. for Equal Rts. v. Fearless Fund Mgmt., LLC*, No. 1:23-cv-03424 (N.D. Ga. 2023).

Companies, and their management teams and boards, should be prepared for increased employment-related litigation including litigation that seeks to hold executive officers and directors personally liable for purported breaches of their fiduciary duties in connection with the corporation's DEI policies.

Companies, and their management teams and boards, should be prepared for increased employment-related litigation including litigation that seeks to hold executive officers and directors personally liable for purported breaches of their fiduciary duties in connection with the corporation's DEI policies.

Because these challenges are so recent, it remains unclear how the *SFFA* holding will specifically be applied to DEI programs that relate to workplace hiring and promotion in the public company context. So while executives and directors may be concerned that a company's DEI policies could expose them to breach of fiduciary duty claims post-*SFFA* relating to "reverse discrimination", they simultaneously cannot ignore the pre-*SFFA* (and continuing) risks of regulatory enforcement actions and litigation alleging discrimination against employees from historically underrepresented minority groups or a corporation's failure to effectively implement and oversee a DEI program and live up to DEI commitments. Over the past three years, approximately 40 lawsuits have been filed alleging failures by companies to protect employees from historically underrepresented minority groups and increase workplace diversity.[3] Several of these were shareholder derivative and federal securities actions alleging that directors violated their *Caremark* oversight duties by, for example, failing to monitor their companies' compliance with anti-discrimination laws, authorizing false statements about the companies' commitment to diversity in proxy statements and other publicly available documents (such as company websites and sustainability reports) and failing to ensure that diverse candidates were selected to sit on the board.[4] Others were discrimination-related suits brought under Title VII of the Civil Rights Act by U.S. agencies or employees from historically underrepresented groups alleging that the companies failed to prevent workplace harassment based on sex, race or religion.[5] There is little reason to believe that *SFFA* will reduce the risk of such litigation, as the Supreme Court was united in acknowledging that discrimination remains a persistent problem that must be addressed. Indeed, Justice Thomas noted in his concurring opinion that he was "painfully aware of the social and economic ravages which have befallen my race and all who suffer discrimination," and Justice Kavanaugh similarly stated in his concurring opinion that "racial discrimination still occurs and the effects of past racial discrimination still persist."

Companies should also keep in mind these additional considerations as DEI programs are reviewed and overseen in the wake of *SFFA*.

— **First**, companies should remain aware of and account for the increasing number of shareholder proposals and proxy advisor and institutional investor guidelines demanding that companies strengthen their commitment to diversity. In the 2023 proxy season, for example, shareholders submitted 29 proposals relating to racial equity/civil

[3] *See* David Hood, "Lawsuits Challenge Corporate Diversity Pledges after Floyd" (April 7, 2023), available here.

[4] *See, e.g., Kiger v. Mollenkopf et al.*, 1:21-cv-00409 (D. Del. Mar. 22, 2021) (derivative suit alleging Qualcomm Inc.'s directors breached fiduciary duties and violated Section 14(a) of the Securities Exchange Act of 1934 by breaking promises to diversify all-white board); *In re Danaher Corp. S'holder Derivative Litig.*, No. 1:20-cv-02846-TNM (D.D.C. Sept. 1, 2020) (derivative suit alleging Danaher's board and CEO made misleading statements about company's commitment to diversity); *Ocegueda v. Zuckerberg*, No. 3:20-cv-04444 (N.D. Cal. July 2, 2020) (derivative suit alleging Facebook's executives and directors breached fiduciary duties and violated Section 14(a) by touting Facebook's commitment to diversity while engaging in discriminatory hiring practices and failing to diversify its board and management); *Esa v. NortonLifeLock Inc.*, No. 5:20-cv-05410 (N.D. Cal. Aug. 5, 2020) (derivative suit alleging NortonLifeLock's board breached fiduciary duties by making misleading statements about commitment to diversity in spite of ongoing discriminatory practices and failure to diversify board and management).

[5] *See, e.g., U.S. Equal Emp. Opportunity Comm'n v. Tesla, Inc.*, No. 4:23-cv-04984 (N.D. Cal. Sept. 28, 2023); *Taylor v. Delta Air Lines, Inc.*, No. 1:22-cv-03130 (N.D. Ga. Aug. 8, 2022).

rights audits; 24 proposals that requested a report on the effectiveness of the company's DEI efforts; 16 shareholder proposals asking for a report on gender or ethnic pay disparities; and 6 proposals asking for a report on the company's board diversity. Overall, diversity and human capital-related proposals received an average of 27.1% of shareholder support during the 2023 proxy season.[6]

— **Second**, institutional investors continue to prioritize diversity and listing exchanges continue to focus on it as well. Blackrock, for example, has stated that U.S. boards should aspire to 30% diversity of membership and encouraged boards to have at least two directors who identify as female and at least one who identifies as a member of an underrepresented group; and Glass Lewis will generally recommend against Russell 3000 Nominating & Governance committee chairs if the board is not at least 30% gender diverse, and against Russell 1000 Nominating & Governance Committee chairs if the board has fewer than one director from an underrepresented community.[7] Nasdaq has also instituted "disclose or explain" rules regarding board diversity, including a rule for Nasdaq-listed companies with six or more directors to (1) have at least one director who self-identifies as female, and at least one director who self-identifies as an ethnic minority or LGBTQ+, or explain why the company does not have at least two directors who self-identify in these categories, and (2) subject to certain exceptions, provide statistical information on the gender, race and LGBTQ+ identification of the board of directors on the company's website, proxy, 10-K or 20-F.[8]

— **Third**, state and federal regulators have also increasingly focused on diversity-related disclosures that are intended to increase transparency for consumers and investors about a corporation's diversity efforts. At the state level, for example, California enacted the VC Diversity Law requiring "venture capital companies" with business ties to California to file annual reports detailing (1) specified demographic data for the founding teams of all portfolio companies invested in during the prior year and (2) the aggregate amounts of investments made by the venture capital company during the prior year and investments in specified categories of portfolio companies. And, at the federal level, the SEC had rulemaking on human capital disclosure on its agenda for the latter part of 2023 and board diversity disclosure on its agenda for early 2024 "to enhance registrant disclosures about the diversity of board members and nominees."[9]

— **Fourth**, a number of credible studies have shown calculable benefits to innovation, culture and the bottom line for companies that make real, sustained efforts to diversify their workplaces and address systemic racism. Numerous studies have shown that businesses that do not consider diversity in their employment programs risk overlooking top talent, reducing innovation, and weakening financial performance.[10] For example, diverse companies tend to be more financially successful than non-diverse companies, as evidenced by a 2020 study showing that companies in the top quartile for diversity and inclusion were 36 percent more likely to show financial results above the median for companies in their industries, and other similar studies that show more diverse companies generally enjoy greater sales revenue and market share, and success in investments

6 Data is from Proxy Analytics. Proposals submitted by anti-ESG proponents are omitted from these statistics.

7 William J. Chudd et al., *Current State of Board Diversity Rules and Policies,* GTDT Practice Guide Diversity and Inclusion 2023 (Aug. 29, 2023).

8 Nasdaq, "NASDAQ's Board Diversity Rule: What Companies Should Know" (Feb. 28, 2023), available here.

9 Office of Information and Regulatory Affairs, Office of Management and Budget, *Human Capital Management Disclosure*, "Corporate Board Diversity", (Spring 2023), available here; For additional information, see our Oct. 2023 blog post available here.

10 *See, e.g.*, Rocío Lorenzo et al., Boston Consulting Group, "How Diverse Leadership Teams Boost Innovation" (Jan. 13, 2018), available here; Erik Larson, Forbes, "New Research: Diversity +Inclusion = Better Decision Making At Work" (Sept. 21, 2017), available here; *HERS Update: Gender Diversity Continues to Drive Alpha*, Morgan Stanley Research (February 1, 2023), quoted in Dean J. Cimino, Morgan Stanley, "Why Gender Diversity May Lead to Better Returns for Investors" (Feb. 2023), available here; Morgan Stanley Research, "Gender Diversity Keeps Paying Dividends" (Mar. 7, 2023), available here.

than less diverse peers.[11] Moreover, research by Deloitte found that promoting all forms of diversity, equity, and inclusion can lead to superior employee engagement and satisfaction, helping a company's bottom line.

Management and boards of companies should be able to articulate their DEI policies and programs, including how they are in the best interest of the company and its stakeholders, aligned with the company's mission and what measurable goals they are intended to achieve.

So, how should management teams and boards be thinking about DEI programs after *SFFA*? Many stakeholders will continue to expect corporations to demonstrate a commitment to and focus on DEI at all levels within the organization, and to follow through on those commitments. Management and boards of companies should be able to articulate their DEI policies and programs, including how they are in the best interest of the company and its stakeholders, aligned with the company's mission and what measurable goals they are intended to achieve. Board oversight is an important element and area of focus in management's ability to create a company's vision on DEI and articulate such vision to investors and other stakeholders in a clear and strategic manner.

Management and boards should also consider the following courses of action:

- Identify measurable and articulable benefits of workplace diversity, including profitability, strategy and benefits to decision-making, and develop programs closely tailored to those benefits. This may include adopting broader approaches to diversity that are more likely to withstand legal scrutiny and connecting DEI programs directly to clearly communicated business goals.

- Assess existing hiring, promotion and DEI policies and values statements in corporate mission statements and trainings to ensure they do not run afoul of how Title VII is likely to be interpreted post-*SFFA*, and set appropriate goals for increasing diversity and inclusion that are relevant to measurable business objectives, to the extent possible; be sure to document these actions and conversations. Though numerical targets can be used to measure progress, they should not be the end goal.

- Review the company's prior public statements and disclosures about diversity to ensure that any policy changes are not inconsistent with past statements.

- Monitor new litigation and regulatory actions relating to discrimination in hiring and promotion practices and keep note of judicial interpretations of *SFFA* in this context.

- Collect and analyze internal data about the results of DEI programs to be able to provide metrics that will help to explain the relevance of the programs to the company's business objectives.

- Increase corporate reporting and controls over DEI programs and disclosures to ensure missed goals or policy violations are promptly flagged to the board.

- At the board level, review and improve committee charters, governance rules and trainings to reflect the company's DEI policies.

[11] *See, e.g.*, McKinsey & Co., "Diversity Wins: How Inclusion Matters" (May 2020), available here; *see also* Vivian Hunt, Dennis Layton & Sara Prince, McKinsey & Co., "Diversity Matters" (Feb. 2, 2015); Vivian Hunt, Sara Prince, Sundiatu Dixon-Fyle & Lareina Yee, McKinsey & Co., "Delivering Through Diversity" (Jan. 2018); BCG, "How Diverse Leadership Teams Boost Innovation" (Jan. 23, 2018); Dieter Holger, Wall Street Journal, "The Business Case for More Diversity" (Oct. 26, 2019), available here; Cedric Herring, 82 AM. SOCIOLOGY REVIEW 868, 876, "Is Diversity Still a Good Thing?" (2017); Paul Gompers & Silpa Kovvali, Harvard Business Review, "The Other Diversity Dividend" (July–Aug. 2018), available here.

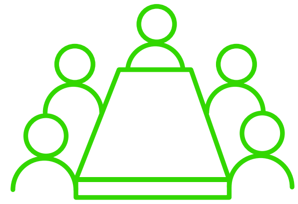
— Foster relationships with investors, clients, customers and other stakeholders that promote collaboration to understand the benefits of and enhance corporate diversity and inclusion.

— Send a message from leadership addressing diversity, but review and consider public statements carefully. Focus on inclusiveness and diversity of perspectives and eliminating bias, and avoid stating that any one protected characteristic offers more value than another.

— Prepare for an impact on the hiring pipeline, including the likely decline in diversity of enrolled students at universities and colleges that may lead to less diversity in job applicant pools and fewer workers from groups that are historically underrepresented to fill vacancies and advance to leadership roles.

In summary, companies should review hiring and promotion practices that account for diversity and corporate DEI programs through the *SFFA*-lens, while ensuring that such review considers the still very real and meaningful litigation and regulatory risks associated with potential discrimination against individuals from historically underrepresented groups. As boards of directors oversee these reviews, they should also be mindful of prior statements the company has made about its DEI programs or hiring and promotion practices and ensure any programmatic changes are consistent with such statements.

Meeting Fiduciary Duties When Speaking Up: A 21st Century Roadmap



Lillian Tsu
Partner
New York
ltsu@cgsh.com

Jonathan R. Povilonis
Associate
New York
jpovilonis@cgsh.com

Companies today face more pressure to speak on social and political issues than ever before. With the constant barrage of issues, the consequences of any course of action can be hard to predict. Speaking up can risk backlash for saying the wrong thing, but refraining from speaking at all may no longer be a reliable way to stay above the fray and avoid criticism. Companies may conclude that, when it comes to issues of great importance to their stakeholders, silence is no longer an option. One question that follows for boards and management, then, is whether they can break the silence without breaching their fiduciary duties.

Consider this now-commonplace scenario: The U.S. Supreme Court issues a ruling that is popular among some stakeholders but is considered morally problematic—perhaps even a cause for great concern—to other stakeholders. It may well be the case that the ruling bears directly on an issue of political significance with little or no obvious direct relevance for businesses or commercial conduct. Nonetheless, it will surprise no one when a company with major domestic operations is bombarded with feedback from its customers and employees expressing outrage at the ruling and demanding that the company take action in response. After much deliberation, the board and management reach a consensus that the company has no choice but to respond—if not to the Supreme Court, then at least to its own customers and employees. Can they do so in a way that is consistent with their fiduciary duties to act in the best interests of the company and its stockholders?[1]

While this is not a question that offers many easy answers, the following guideposts will help companies navigate this new terrain.

[1] This memo describes the law in the State of Delaware, the state in which most Fortune 500 companies are incorporated. While many states look to Delaware as an authority on issues of corporate law, companies that are incorporated in other states should consult with local counsel to ensure that any relevant differences are taken into consideration.

Take Account of Stakeholders

As with any decision, the guiding light for a company's board and management should be the best interests of the company and its stockholders.[2] This does not mean, though, that a company is required to respond to political or social issues like controversial court rulings with a myopic view toward immediate stockholder return.[3] Courts have acknowledged that corporate fiduciary duties leave sufficient room for the board and management to consider the interests of non-stockholders like employees, customers and local communities, so long as these considerations are rationally related to the protection of long-term stockholder value.[4]

As companies continue to face both ESG issues and the backlash against them, they will do well to keep both stockholder and non-stockholder perspectives top of mind. For issues that are significant to the company as a whole, directors and officers can fulfill their fiduciary duties by actively engaging the issues. The task with each significant issue is to give it due consideration by weighing the key risks involved.

For issues that are significant to the company as a whole, directors and officers can fulfill their fiduciary duties by actively engaging the issues. The task with each significant issue is to give it due consideration by weighing the key risks involved.

A company in the consumer goods sector may feel the most pressure to take action on topics that are meaningful to its customers, while an industrials company with predominantly commercial clients may determine that its relations with employees would suffer the most harm if the company declined to respond publicly on topics of importance to that constituency. A company's standing in the surrounding communities can be equally important to consider, as can its reputation among politicians and regulators at the local, state and national levels. No company can succeed in the long run if it does not maintain good relations with each group of stakeholders, so there is often ample opportunity to draw the connection to long-term stockholder value. Of course, this is only the first step as difficult trade-offs must often be made in the near term, but weighing the key risks is exactly the sort of deliberations that a board should undertake when the company's voice is used on significant matters for the company, including important ESG matters.

Consider Current Market Practice

Fortunately, the scenario described above is one in which the law affords significant latitude to directors and officers to rely on their experience with the company's core constituencies in balancing their various interests. Unlike a corporate takeover scenario in which a court would evaluate board and management decisions with varying levels of heightened scrutiny, a company's response to changes in law and other ESG issues in the ordinary course of business will typically be protected by application of the business judgment

---

2 See, e.g., *Revlon, Inc. v. Macandrews & Forbes Holdings, Inc.*, 506 A.2d 173, 181 (Del. 1986) (stating that fiduciary duties "require the directors to determine the best interests of the corporation and its stockholders, and impose an enhanced duty to abjure any action that is motivated by considerations other than a good faith concern for such interests.") (citing *Unocal Corp. v. Mesa Petroleum Co.*, 493 A.2d 946, 954 (Del. 1985). See also Leo E. Strine, Jr., *The Dangers of Denial: The Need for a Clear-Eyed Understanding of the Power and Accountability Structure Established by the Delaware General Corporation Law*, 50 Wake Forest L. Rev. 761, 768 (2015) ("[A] clear-eyed look at the law of corporations in Delaware reveals that, within the limits of their discretion, directors must make stockholder welfare their sole end, and that other interests may be taken into consideration only as a means of promoting stockholder welfare").

3 See, e.g., *Simeone vs Walt Disney Co.* 302 A.3d 956, 958–959 (Del. Ch. Jun. 27, 2023) [hereinafter *Disney*] ("Delaware law vests directors with significant discretion to guide corporate strategy—including on social and political issues. Given the diversity of viewpoints held by directors, management, stockholders, and other stakeholders, corporate speech on external policy matters brings both risks and opportunities. The board is empowered to weigh these competing considerations and decide whether it is in the corporation's best interest to act (or not act).")

4 *Id.* at 182 ("A board may have regard for various constituencies in discharging its responsibilities, provided there are rationally related benefits accruing to the stockholders.") (citing *Unocal*, 493 A.2d at 955). See also *Disney*, 302 A.3d at 971("The Board's consideration of employee concerns was not, as the plaintiff suggests, at the expense of stockholders. A board may conclude in the exercise of its business judgment that addressing interests of corporate stakeholders—such as the workforce that drives a company's profits—is "rationally related" to building long-term value. Indeed, the plaintiff acknowledges that maintaining a positive relationship with employees and creative partners is crucial to Disney's success.")

rule.[5] So long as the corporate decisionmakers are disinterested and independent (*i.e.*, so long as they do not stand to derive any personal financial benefit from the decision), a court will defer to their judgments that are made in good faith absent unusual circumstances.[6]

Even with the latitude provided by the business judgment rule, though, making trade-offs among the company's stakeholders is no easy task. The loudest voices are often singularly focused, and ignore the balancing act of opposing stakeholder interests that must be performed with any corporate decision. A steadier measure of how any decision will be judged is current market practice of the company's peers and competitors.

If a controversial ruling puts a company's employees in a significantly worse position than the one they were in previously, it is likely that other domestic companies are facing a similar predicament. The company's decision to fund its employees' travel to surrounding states in attempt to shield them from the worst consequences of the ruling, for example, will look much less extreme if several of the company's main competitors are offering the same benefit. Instead, it may well be the bare minimum that is required for the retention of key employees that are needed to meet production targets. On the other hand, if the response called for by the company's harshest critics has not been put into practice by any of the company's peers, it is probably an indicator that there is less urgency in issuing a response.

Speak to Core Values

When companies do decide to speak on a controversial issue, they tend to tread carefully. But one thing that is often overlooked in the rush to get out a response is that inauthentic or insincere statements will ring false for everyone, even those that agree with them. On the other hand, companies that speak to their longstanding core values can often endure their harshest critics—as well as a court—even on issues for which consensus is hard to find.

Directors and officers that can link the company's response to the values that are already driving the company's success will have the highest likelihood of achieving the desired outcome

Making an authentic statement on behalf of a company is a tall order, and typically requires a deep familiarity with the company's brand, reputation and recent track record. This is where the business judgment of the board and management has its most utility. Directors and officers that can link the company's response to the values that are already driving the company's success will have the highest likelihood of achieving the desired outcome.[7] The company's stockholders, customers and employees are already on board with the company's mission, at least to some extent, and sincere statements that align with that will have the highest chance of maintaining their continued loyalty and commitment.

5 See, e.g., *Brehm v. Eisner*, 746 A.2d 244, 264 (applying the business judgment rule in a suit challenging a president's employment agreement and holding that "Courts do not measure, weigh or quantify directors' judgments. We do not even decide if they are reasonable in this context. Due care in the decisionmaking context is process due care only. Irrationality is the outer limit of the business judgment rule. Irrationality may be the functional equivalent of the waste test or it may tend to show that the decision is not made in good faith, which is a key ingredient of the business judgment rule.").

6 See, e.g., *Sinclair Oil Corp. v. Levien*, 280 A.2d 717, 720 (Del. 1971) ("A board of directors enjoys a presumption of sound business judgment, and its decisions will not be disturbed if they can be attributed to any rational business purpose. A court under such circumstances will not substitute its own notions of what is or is not sound business judgment.").

7 To borrow an example from the takeover context, in *Paramount Communications v. Time*, the Supreme Court of Delaware held that the Time directors had acted in accordance with their fiduciary duties because, after an informed investigation, they concluded in good faith that their chosen course of action was the "best 'fit' for Time to achieve its strategic objectives" and allowed for "the preservation of Time's 'culture,' i.e., its perceived editorial integrity in journalism." 571 A.2d 1140, 1142 (Del. 1989). But see *eBay Domestic Holdings, Inc. v. Newmark*, 16 A.3d 1, 33 (clarifying that "*Time* did not hold that corporate culture, standing alone, is worthy of protection as an end in itself" and that "[u]ltimately, defendants failed to prove that [their company] possesses a palpable, distinctive, and advantageous culture that sufficiently promotes stockholder value to support [the challenged decision,] the indefinite implementation of a poison pill.").

Integrate into Long-Term Success

The last step is perhaps the most important. Companies that speak on controversial issues will do well to expect at least some backlash—and to remember that backlash is something that can be managed. There are ways to increase the chances that the company's chosen course of action will be upheld, both in a court of law and in the court of public opinion. The company's board and management should think carefully to find ways in which the company's response to a controversial issue can be integrated into the company's practices and memorialized in the company's policies.

Employees that believe their dignity will be protected by the company are less likely to leave for a competitor, and customers that believe in the company's mission will return to the company when it is time to make another purchase. But, even more importantly, no company wants to become the scapegoat of politicians, commentators or plaintiffs' attorneys, especially those that have an axe to grind. The best way to avoid this outcome, or to limit its negative impact, is to ensure that the company's response to any high-visibility issue is directly justified in relation to the company's longstanding commercial goals and achievements. And the best way for directors and officers to protect themselves in the face of stockholder litigation is give each significant issue due consideration when it arises.

It may be obvious to the board and management how their decision will promote the best interests of the company and its stockholders. And while the business judgment rule should protect decisions of this nature from undue interference by the courts, in the "20/20 hindsight" world of stockholder litigation, it never hurts to spell out what is otherwise an inference.

Conclusion

Speaking out on controversial issues is a daunting task, yet companies are being called to do so more and more. While the potential for foot faults abound, directors and officers who are guided by the above principles can fulfill their fiduciary duties and avoid the worst consequences of entering the political fray.

Outlook for M&A and Shareholder Activism in 2024

James E. Langston
Partner
New York
jlangston@cgsh.com

Kyle A. Harris
Partner
New York
kaharris@cgsh.com

The M&A Environment in 2024

Global deal value in 2023 fell to the lowest level seen in a decade. It was the first year since 2013 that the M&A market failed to hit the $3 trillion value mark, with continued reduced deal activity from private equity firms, which spent 36% less on acquisitions than in 2022. For boards and management teams pondering the M&A environment in 2024, a complex mix of macroeconomic, geopolitical and sector-specific headwinds and tailwinds make prognostication difficult.

Such a complex transactional environment provides challenges but also opportunities. From our vantage point, the number of transactions being actively considered is much higher than the relatively depressed 2023 metrics imply, suggesting many deal-makers are not deterred. Below are some key themes from 2023 and lessons for 2024.

The cost of capital will remain elevated relative to pre-pandemic levels for some time and further valuation resetting is likely necessary to bridge the gap between many buyers and sellers, particularly in leveraged transactions.

Among other sources of friction, the biggest barrier to M&A has been the slowly narrowing but still lingering valuation gap between buyers and sellers in many sectors, which has been exacerbated by the increased cost of capital. In the U.S., the latter appears to be on a path to stabilizing, as a consensus emerges that interest rates have likely peaked, with Federal Reserve policymakers signaling potential rate cuts by the end of 2024. While this bodes well for acquisition financing and deal making generally, the cost of capital will remain elevated relative to pre-pandemic levels for some time and further valuation resetting is likely necessary to bridge the gap between many buyers and sellers, particularly in leveraged transactions.

On the other hand, portfolio reshaping remains a significant driver of transactions, as corporates look for opportunities to reposition strategically and to separate high-growth from low-growth assets and achieve multiple re-ratings. Various sources of industry disruption—from re-shoring or near-shoring to address supply chain vulnerabilities, to energy transition, digitalization, and the adoption of artificial intelligence—will also continue to spur transactions.

Private equity firms are starting the year with a record amount of dry powder, which seems to have become an annual refrain. They are also sitting on a record backlog of portfolio company exits, putting firms under greater pressure to return capital to limited partners. At some point, valuations will further reset and private equity's share of the market will recover, greasing the skids for deal making overall. Until then, we expect private equity sellers to rely on more structured transactions to bridge valuation gaps—including use of performance-based earn-outs or other contingent consideration, seller financing, and larger equity rollovers—and for private equity buyers to seek opportunities for take-privates and from corporate de-conglomeration and portfolio optimization.

The headlines tend to overstate the risk for clearing many deals, including those with regulatory complexity, provided the parties have a well-considered and well-executed strategy, which requires seamless coordination among M&A, antitrust and foreign investment lawyers who understand the new playbook (and how to deploy it and where to diverge from it).

Heightened regulatory scrutiny of transactions will remain top of mind for companies and investors seeking to transact in 2024. High profile, and in some cases unpredictable, merger enforcement has likely had its intended deterrent effect. Yet we believe the headlines tend to overstate the risk for clearing many deals, including those with regulatory complexity, provided the parties have a well-considered and well-executed strategy, which requires seamless coordination among M&A, antitrust and foreign investment lawyers who understand the new playbook (and how to deploy it and where to diverge from it).

2023 also demonstrated that an increasingly broad spectrum of investors, beyond traditional activists, are more willing to weigh in on announced deals and M&A strategy—a trend which will certainly continue in 2024. This places a premium on corporate messaging prior to, at, and following announcement.

Shareholder Activism Outlook

On the shareholder activism front, 2023 saw more M&A-focused demands than observers might have expected for such a down year in the M&A and financing markets. These campaigns predominated at small-cap issuers and fund complexes, however, with larger cap campaigns more focused on operational improvements, portfolio reshaping and capital allocation. CEOs also increasingly found themselves in activists' cross-hairs. We expect this bifurcation to continue early in 2024 but would expect the push for M&A to accelerate if financing and M&A markets improve over the course of the year.

In the U.S., 2023 was also a noticeably litigious proxy season. Many U.S. issuers seized the occasion of universal proxy implementation to enhance nomination requirements under their advance notice bylaws. In some cases, these amendments included particularly stringent disclosure requirements for nominating stockholders. Companies were also increasingly willing to challenge the validity of nominations, whether under newly adopted or preexisting bylaws. These developments were met with an increase in litigation challenging such bylaws and nominee rejections. In situations involving the most aggressive bylaws or other overly restrictive tactics, these lawsuits generally resulted in settlements with the activist, which provided for appointment of some portion of the activist slate or allowing the activist's nominees to stand for election.

The year also saw an increase in bespoke terms for settlement agreements. In addition to customary commitments on board and committee composition, a number of settlements included more tailormade features, including changes to organizational documents (including modifications to the rights of existing controlling stockholders or roll-back of advance notice bylaws) and more prescriptive terms for dividend or share repurchase programs.

In preparing for activism in 2024, boards and management teams should consider the following lessons from 2023:

— Strong defensive tactics will continue to have their place in the corporate playbook. But frequently, in the current environment, the use of overly aggressive maneuvers to thwart nominations runs the risk of being poorly received by shareholders, resulting in tarnished incumbents and victorious activists. The best defense begins before the activist emerges, in staying close to shareholders, conducting outside-in reviews of governance and performance, and preemptively addressing potential vulnerabilities or developing communication plans to explain them. When an activist emerges, the most likely path to success is to engage on the merits. Companies should rebut activist demands that are misguided but consider preempting demands, where possible, with actions that are likely to be supported by shareholders.

— Corporations that have not already done so should still consider review of their bylaws to reflect the state of the art in advance notice provisions. But in adopting any amendments, boards and management should be mindful of the increasing scrutiny applied to these bylaws from shareholders, activists and proxy advisors, and be ready to explain how they protect shareholder rights and the integrity of the franchise.

— The advent of universal proxy in the U.S. and the ability of shareholders to pick and choose between slates will result in the continued personalization of election contests, with activists focusing on directors perceived to be most vulnerable. Companies should review their board evaluation and refreshment policies and their disclosure regarding director qualifications, contributions, and board effectiveness.

— Corporations should expect more onerous settlement demands from activists and, in considering these terms, be mindful of the reaction of other shareholders.

— Heightened M&A scrutiny from investors, whether in the form of "bumpitrage" or "breakitrage" campaigns from traditional activists or vocal opposition from institutional investors, is here to stay. Companies should revisit their ongoing disclosure to ensure M&A strategy is properly articulated, to avoid investor surprise, and carefully consider announcement materials to proactively communicate the merits of a transaction and preempt potential critique.

Crossing a New Threshold for Material Cybersecurity Incident Reporting

Helena K. Grannis
Partner
New York
hgrannis@cgsh.com

Rahul Mukhi
Partner
New York
rmukhi@cgsh.com

Jonathan S. Kolodner
Partner
New York
jkolodner@cgsh.com

Tom Bednar
Counsel
Washington, D.C.
tbednar@cgsh.com

Nina E. Bell
Senior Attorney
New York
nbell@cgsh.com

James P. Abate
Associate
New York
jabate@cgsh.com

In July 2023, the U.S. Securities and Exchange Commission (SEC) adopted final rules to enhance and standardize disclosure requirements related to cybersecurity. In order to comply with the new reporting requirements of the rules, companies will need to make ongoing materiality determinations with respect to cybersecurity incidents and series of related incidents. The inherent nature of cybersecurity incidents, which are often initially characterized by a high degree of uncertainty around scope and impact, and an SEC that is laser-focused on cybersecurity from both a disclosure and enforcement perspective, combine to present registrants and their boards of directors with a novel set of challenges heading into 2024.

In addition to requiring certain annual disclosures relating to cybersecurity risk management, strategy and governance, the final rules added Item 1.05 to Form 8-K, requiring domestic registrants to disclose any material cybersecurity incident[1] within four business days after a registrant determines that it experienced such an incident (the final rules also amended Form 6-K to add "cybersecurity incidents" as a reporting topic for foreign private issuers). Now effective for most domestic registrants, new Item 1.05 requires registrants to describe the (i) material aspects of the nature, scope and timing of the incident and (ii) material impact or reasonably likely material impact on the registrant, including on its financial condition and results of operations (new Item 1.05 Form 8-K disclosure will be required for smaller reporting companies starting June 15, 2024). Registrants must also provide updates by filing amended Form 8-Ks to the extent certain information remains unknown at the time of the initial filing.

While registrants generally have well-established disclosure controls and procedures to make sure that required Form 8-K items are disclosed in a timely manner, new Item 1.05 is unique in that the disclosure trigger is the determination of materiality, rather

[1] The final rules define a "cybersecurity incident" as "an unauthorized occurrence on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein."

Suggested Factors for Consideration:

— **Potential economic losses**

- Does the cybersecurity incident or response affect operations in a way that has materially affected, or is reasonably likely to materially affect, the company's financial performance, result in a revenue loss or impact on goodwill?
- Has the cybersecurity incident materially affected, or is it reasonably likely to materially affect, the company's financial position as a result of adverse costs (including misappropriation of company assets), incident response-related fees (including ransomware payments) or fees for increased cybersecurity defense or insurance?
- Will the company have to spend additional resources to retain existing or obtain new customers or suppliers as a result of this cybersecurity incident?

— **Scope of the incident and impact on key systems**

- How many individuals were affected, if there is a data breach?
- Is the company's access to key data or systems compromised?
- Does the incident suggest a potential ongoing security vulnerability?
- Does the incident suggest or result in any significant deficiencies or material weaknesses in the internal control over financial reporting, or implicate disclosure controls and procedures?

— **Impact on data**

- Was data compromised that relates to business interruption or network security?
- What is the overall sensitivity/proprietary nature of any such compromised data?

— **Incident response**

- How quick and how effective were the company's controls in identifying and responding to the incident?
- How quickly does the company expect to recover normal operations?

— **Legal consequences and reputational harm**

- What is the likelihood of civil litigation or regulatory enforcement actions?
- What is the potential for reputational harm?
- Does the incident expose the company to customer-related disputes including returns, warranty claims or litigation?

than the underlying event itself, and provides that the determination of materiality is required to be made without unreasonable delay. We expect the impact of anticipated SEC and investor scrutiny of disclosure determinations to cause companies to consider disclosure of events even before a final determination of materiality has been made. Below we discuss some key takeaways and governance considerations in light of the new required Form 8-K disclosure.

Incident Materiality Analysis

In preparation for the materiality determinations that will be required, registrants should ensure their systems and controls for responding to and evaluating cybersecurity incidents address the need for potential disclosure. Cybersecurity incident response plans should contemplate involving internal legal departments early and often in order to make sure that materiality and disclosure obligations are considered repeatedly as a situation develops. Prompt consultation with external advisors, including cybersecurity experts, auditors and outside counsel is also generally advisable. Processes must also be in place to enable aggregation of individual incidents and to perform an aggregated materiality analysis, also on a potentially continuing basis.

Consistent with general disclosure principles and caselaw, information is material if "there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision, or if it would have "significantly altered the 'total mix' of information made available" – the SEC has reiterated that it did not create or intend to create a new materiality standard for cybersecurity.

Above, we provide a list of questions that registrants may wish to consider, among others, when evaluating quantitative and qualitative factors to address the materiality of a cybersecurity incident, bearing in mind that materiality determinations must consider the total mix of information and no individual factor would necessarily be dispositive.

Disclosure Timing Considerations

Given the number of moving pieces and factors to consider, it is likely that it may take some time to reach a definitive conclusion around materiality for any given cybersecurity incident. If a registrant waits until it has come to a final conclusion around materiality, a significant amount of time may have passed since the initial discovery of the incident. The SEC has been extremely focused on the timeliness of disclosure of cybersecurity incidents, and while an incident may appear to be immaterial for some period of time and non-disclosure at that time would be technically compliant with the disclosure rules, if the incident is later determined to be material, there is likely to be a tremendous amount of scrutiny around the timing of that determination.

One of the benefits of initially utilizing Items 7.01 or 8.01 instead of Item 1.05 is that there is no preemptive concession by the registrant of the event's materiality in a potential future litigation or otherwise.

As a result, registrants will want to think carefully about the potential benefits of putting out disclosure on Form 8-K under Item 7.01 (Regulation FD Disclosure) or Item 8.01 (Other Events) (and/or in a press release or other Regulation FD-compliant channel) promptly after discovering a cybersecurity incident, while the materiality of the incident is still under consideration (including if they do not believe the incident will likely be deemed material). In addition to the disclosure technicalities, one of the benefits of initially utilizing Items 7.01 or 8.01 instead of Item 1.05 is that there is no preemptive concession by the registrant of the event's materiality in a potential future litigation or otherwise. In some circumstances, disclosure more quickly than the usual four day Form 8-K deadline will be appropriate. We have seen an increasing number of registrants adopt this practice, even ahead of the

Item 1.05 requirement becoming effective, and believe it can be an effective communication tool, while also mitigating regulatory and other risk. By disclosing early, a registrant will give itself some breathing room to come to a materiality determination in an expeditious but methodical way that considers all necessary factors. In addition, providing prompt disclosure may provide some protection from stock-drop lawsuits following a potential later announcement that the incident has been determined to be material.

Additionally, registrants may need to alert and provide ongoing updates to certain external stakeholders. For example, registrants may need to coordinate logistics with vendors if their systems are inaccessible, or may be unable to meet their immediate obligations to customers due to production or operational issues. These types of issues will necessitate real-time engagement with impacted constituencies. Putting out public disclosure will facilitate this dialogue and alleviate any concerns around claims of selective disclosure in violation of Regulation FD.

We expect that the developing practice of making an initial disclosure on Form 8-K under Item 7.01 or 8.01 (and/or by press release or other Regulation FD-compliant channel) will likely continue, as registrants will not want to commit themselves to Item 1.05 disclosure and the related materiality determination and resulting additional requirements until they have had time to fully assess the situation. Whether Item 7.01 or Item 8.01 is appropriate (the latter of which carries with it an implicit element of materiality and is filed, not furnished) will be a facts and circumstances determination.

Prepare for Subsequent Inquiries

Many registrants that have disclosed cybersecurity incidents have received later inquiries from the SEC. These inquiries have focused on what was known and when, how the incident was detected, whether the registrant was aware of vulnerabilities that were exploited, whether the registrant engaged with the bad actor, the registrant's process and considerations around disclosure and whether there were any implications for internal controls.

Registrants will want to document their materiality assessment at multiple junctures in the process, as well as keep a high-level record of the overall timeline for the incident and response, to be able to respond to these inquiries.

In responding to any cybersecurity incident, registrants should assume that regulators may ask detailed questions after the fact. As a result, registrants will want to document their materiality assessment at multiple junctures in the process, as well as keep a high-level record of the overall timeline for the incident and response, to be able to respond to these inquiries. In some instances, preparing SAB 99 materiality analyses may be warranted, particularly if financial systems and/or controls are implicated in the incident.

Lessons from SolarWinds

When considering disclosure issues around cybersecurity, registrants should take heed of the lessons from the recent charges filed by the SEC against the software company SolarWinds. In October, 2023 the SEC charged the company and its CISO with allegedly misleading investors about its cybersecurity practices and known risks. The SEC's case is built on contrasting public disclosures touting the company's supposedly strong cybersecurity practices with allegedly inconsistent internal documents that painted a much bleaker picture regarding the adequacy of its defenses. In addition to alleging that the company included "only generic and hypothetical cybersecurity risk disclosures" that failed to address known, specific risks, the SEC also alleges that when the company did eventually publicly disclose a cybersecurity incident, its disclosure was inadequate because it did not disclose that threat actors had already exploited certain known vulnerabilities multiple times, despite management's awareness of these incidents.

In the SolarWinds complaint, the SEC made clear its view that registrants must have disclosure controls that cause management to consider the disclosure ramifications of cybersecurity vulnerabilities and intrusions, and for the first time stated its view that a company's required system of internal controls must include cybersecurity controls that are adequate to ensure that third parties cannot access company assets.

Registrants should make sure that public statements about cybersecurity matters, including the disclosure of any cybersecurity incidents (and the annual disclosure required by other elements of the SEC's cybersecurity disclosure rule), are carefully reviewed for alignment with company knowledge about the extent of the incident at the time disclosure is made, to make sure the registrant is not understating the known severity, and with the company's internal assessments of its defenses and risks, to make sure the registrant is not overstating the adequacy if its defenses.

Board Oversight and Key Takeaways for Boards of Directors

To make sure a company is ready to address any cybersecurity incident, boards of directors (and delegated committees) should:

— Receive regular reports on cybersecurity risk from management and outside advisors. Directors should actively deliberate, ask questions, engage in discussions and challenge proposed courses of action, including by engaging external advisors when appropriate.

— Confirm that management regularly updates and tests cybersecurity incident response plans and cybersecurity policies.

— Confirm that plans and policies include disclosure controls and procedures that force management to consider whether cybersecurity incidents, individually or in the aggregate, warrant disclosure.

— Oversee the implementation of disclosure controls and procedures that are reasonably designed to facilitate or ensure that cybersecurity-related disclosure is reviewed by appropriate members of management for accuracy.

— Regularly review the company's cybersecurity budget to ensure appropriate resources are available, understand where capital is being directed for defense and remediation of systems and assess cyber insurance coverage.

— Make sure that board and committee minutes and other formal board records adequately document the board's and committee's discussions of cybersecurity, including any incidents, as well as any internal or external subject matter experts consulted, as it is increasingly common in shareholder derivative suits for the plaintiff to request minutes and other documents from the company and then use those documents to craft a complaint.

While management should ultimately be making any materiality determinations and driving the day-to-day incident response, the board should be involved in the oversight of this process.

Upon discovery of a potentially significant cybersecurity incident, companies should promptly alert and involve the appropriate constituency within the board of directors. Depending on the company, this is likely to be the committee to whom responsibility for the oversight of cybersecurity matters has been delegated, or the chair of that committee. Periodic, high-level updates should also be given to the full board of directors. While management should ultimately be making any materiality determinations and driving the day-to-day incident response, the board should be involved in the oversight of this process.

In particular, once a significant cybersecurity incident is discovered, the board should:

— Oversee management's response to the incident.

— Discuss management's disclosure approach, including disclosure to the market, customers, regulators and other stakeholders.

— Consider and evaluate the broader implications of any cybersecurity incidents, including:

  - Whether there are any implications for the company's disclosure controls and procedures and internal control over financial reporting, including whether these are still effective; and

  - Whether the incident was anticipated by the company's cybersecurity defense and implications for the company's cybersecurity risk management processes as a whole.

— Consider the implications for cybersecurity defense funding going forward, include as this relates to cybersecurity insurance.

— Review and debrief with management on post-incident remediation.

— Review the company's cybersecurity risk management program and cybersecurity incident response plan to consider lessons learned and appropriate updates.

— Consider the longer-term disclosure implications, as any cybersecurity incidents will inform cybersecurity-related disclosure in future annual reports, including in response to the new rules and in risk factors, on which board members have liability.[2]

Conclusion

SEC attention to and scrutiny of cybersecurity disclosure and internal risk analysis is likely to increase under the new reporting regime. In this brave new world of regulation and with the frequency of cybersecurity incidents only increasing, it remains imperative that boards focus their attention on a company's system and controls for not only responding to cybersecurity incidents, but also evaluating disclosure obligations with respect to such incidents.

2 For further discussion of cybersecurity disclosure in annual reports, *see* our August alert memo available here.

A New Season for Executive Compensation Disclosure

Michael J. Albano
Partner
New York
malbano@cgsh.com

Audry X. Casusol
Partner
New York
acasusol@cgsh.com

Julia L. Petty
Partner
New York
jlpetty@cgsh.com

Laura Bagarella
Counsel
New York
lbagarella@cgsh.com

Ariel Adler
Associate
New York
aradler@cgsh.com

Gretchen Dougherty
Associate
New York
gdougherty@cgsh.com

Executive compensation issues may not have been the predominant focus for boards of directors in 2023 given the enhanced attention to antitrust, diversity and climate reporting matters, among others. However, there have been several notable developments in executive compensation that boards should be mindful of in 2024. We discuss these developments below.

Pay Versus Performance Considerations for the 2024 Proxy Season

Now that the 2023 proxy season has come to an end, most companies have already complied with the Securities and Exchange Commission's (the SEC) new rules requiring disclosure of various "pay versus performance" metrics in their annual proxy statements (the PVP Rules).[1] We look back at the first PVP Rule disclosures to highlight trends and developments, all with an eye toward preparation for the upcoming 2024 proxy season.

— **Start the Process Early** – By now, most companies are aware of how time-consuming it can be to determine methodologies and track and value equity-based awards and pension benefits for purposes of determining "compensation actually paid" (CAP) in order to comply with the prescriptive requirements of the PVP Rules. It is important to understand that compiling the information necessary to comply with the PVP Rules will likely require coordination amongst a multi-disciplinary team (including HR, legal and finance). It is best to start this process as early as possible so as to be able to gather the relevant information, work with internal constituents and external advisors as appropriate and address any issues that may arise along the way.

As predicted, the vast majority of PVP Rule disclosures have been exercises in disclosing the bare minimum necessary to comply, with many companies opting for simple graphs and charts in lieu of lengthy narrative discussions.

— **Less is More (For Now at Least)** – As predicted, the vast majority of PVP Rule disclosures have been exercises in disclosing the bare minimum necessary to comply, with many companies opting for simple graphs and charts in lieu of lengthy narrative discussions. According to an FW Cook Report of S&P 500 companies, the overwhelming majority of companies (91%) used graphs or charts to describe the relationship between the CAP of the primary executive officer (PEO) and other named executive officers (NEOs) and the company's total shareholder return (TSR), net income and "company selected measure" (CSM), while the remaining 9% used a narrative only description.[2] This trend, however, could change as institutional investors and proxy advisory firms now have had one round of disclosure analysis under their belts and may seek to more systematically integrate these disclosures into their voting analyses and models, which could impact the bare minimum approach companies have taken to date. This is not to suggest that companies should proactively seek to expand on their disclosures, but rather make sure to monitor developments should a shift in practice begin to emerge due to the pressures of these constituents.

— **Simplicity** – Similarly, companies overwhelmingly have opted to use a published line-of-business or industry index as their TSR comparator group, as opposed to a customized peer group used by the company for compensation-related decisions. This was largely due to the simplicity in being able to rely on a published index, which minimizes the need to recalculate disclosures (as would be the case with a custom peer group that changed over time). According to the FW Cook Report, 76% of companies used their 10-K published line-of-business or industry index as their TSR comparator group.[3]

— **Choose Wisely** – Many companies spent time debating the proper CSM. Choosing the CSM is a very company-specific task and should focus on the measure that is most important to linking the company's pay to its performance. Typically, this would be the most prominent measure the compensation committee uses when designing its performance-based compensation. For example, if 90% of incentive pay for a company's executives is tied to EBITDA while 10% is tied to relative TSR, it

1 The PVP Rules apply to U.S. public companies subject to SEC reporting (other than foreign private issuers, most registered investment companies and emerging growth companies) and generally require disclosure in proxy or information statements in which disclosure under Item 402 of Regulation S-K is required with respect to any fiscal year ending on or after December 16, 2022. For further detail on the PVP Rules, see our September 2022 alert memo, available here.

2 FW Cook, "Observations From S&P 500 Pay Versus Performance Disclosures" (June 13, 2023), available here.

3 FW Cook, *supra note 2*.

would likely make more sense to use EBITDA instead of TSR as the CSM. In our experience, the most commonly selected measures were EBITDA, EPS and revenue-based measures. There was initially some uncertainty around the question of whether relative TSR could be used as a CSM, though the SEC has since clarified that relative TSR is a permissible metric for the disclosure – setting the stage for a potential uptick in its usage in this upcoming proxy season.

— **Let the SEC be Your Guide** – The SEC's comment letters on companies' initial pay versus performance disclosures provide insight into the SEC's primary areas of focus. The SEC's comment letters related to calculation inconsistencies, incomplete or missing disclosures (*e.g.*, missing the breakdown of equity adjustments to calculate CAP or failure to identify each NEO included in the calculation of average non-PEO compensation) or presentation problems, such as incorrect table headers or descriptions. Companies should be careful to ensure any disclosures in their 2024 proxy statements are clear and in technical compliance with the PVP Rules. The SEC also released new Compliance and Disclosure Interpretations (C&DIs) regarding the PVP Rules. While fairly technical, the C&DIs deal with topics such as valuation methodologies, treatment of unvested awards modified in connection with a restructuring, the change in fair value of awards granted before an IPO and the meaning of "vesting" for purposes of calculating CAP for awards that either have retirement conditions, conditions requiring compensation committee certifications, market conditions or awards that fail to meet vesting conditions. When preparing their 2024 proxy statements, companies should review the new C&DIs to ensure their disclosures are consistent with the SEC's guidance.

— **Advisory Firm Guidelines** – We recommend monitoring institutional shareholder and proxy advisory firm policies for their guidelines regarding how they evaluate pay versus performance. In its 2024 guidelines, Glass Lewis revised its discussion of its pay-for-performance analysis to note that the disclosure required by the PVP Rules may be used as part of its supplemental quantitative assessments supporting its primary pay-for-performance grade.[4]

Clawbacks: From Adoption to Practice

By now, companies should have implemented clawback polices that are compliant with SEC and national stock exchange rules requiring the mandatory clawback of incentive-based compensation in the event of an accounting restatement (the Clawback Rules).[5] But adoption of a compliant policy is not the end of the road. With delisting potentially at stake for failure to comply with the Clawback Rules, below are some steps companies should take to ensure compliance with the Clawback Rules going forward and to address uncertainties in the SEC and listing exchanges' interpretations of the rules.

Filings and Disclosure

— Companies are generally required to file their clawback policy as an exhibit to their next annual report on Form 10-K, 20-F or 40-F, as applicable.

— Companies should review their compensation disclosure for upcoming proxy statements with the Clawback Rules in mind. This is particularly important given the inherent tension between demonstrating an alignment between executive compensation and financial performance, which will remain a focus of shareholders and proxy advisory firms, and linking elements of compensation that the compensation committee did not intend to be "incentive compensation" within the meaning of the Clawback Rules (*i.e.*, base salary increases), but that might be deemed performance-based if the disclosure suggests it is contingent or related to attainment of financial performance metrics.

4 Glass Lewis, "2024 Benchmark Policy Guidelines: United States," available here.

5 See our November 2022 alert memo for further detail on the Clawback Rules, available here, as well as our October 2023 blog post on common clawback questions, available here.

Companies should consider adopting internal governance structures to advise on specific actions the company would need to take for accounting restatement-related matters, either regularly or in connection with a particular triggering event.

Governance and Controls

— In order to be fully prepared in the event of an accounting restatement, companies should consider adopting internal governance structures to advise on specific actions the company would need to take for accounting restatement-related matters, either regularly or in connection with a particular triggering event. This could include delegating tasks to specific committees, executives or third party advisors.

We expect many compensation committees to work with their compensation consultants and advisors in structuring or modifying compensation programs with an eye toward enforcement of the Clawback Rules and potential mitigation of the effect of new clawback policies on executives' compensation.

— In addition to adopting new governance structures, compliance with the Clawback Rules will require more fulsome internal controls and procedures, including documentation and decision-making processes for determinations regarding compensation (*e.g.*, preparing materials for compensation committee meetings, including significant detail regarding the role of financial/non-financial metrics considered by the committee when making compensation decisions). Companies should clearly delineate which items of compensation may be subject to the Clawback Rules and evaluate whether certain elements of their compensation programs may be inadvertently covered by the Clawback Rules due to being awarded partially in recognition of prior achievement of financial reporting measures, even if the compensation itself is not subject to further achievement of financial goals. Having a clear record of methodology at the outset may help to quantify the appropriate amount to recover and preserve maximum flexibility in the event a clawback is triggered.

Review of Compensation Programs and Plan Design

— Companies should review their current compensation arrangements and evaluate whether and how current contracts will need to be modified to address the Clawback Rules and to assess the feasibility of recovery in the event a clawback is triggered. This review should include ensuring awards and contracts with executive officers include clawback language that could be unilaterally used by the company to permit recovery as required under the Clawback Rules, or that at least reference any clawback policies adopted by the company. In addition, for future annual equity or bonus awards, companies should consider whether to require executives to execute, as a condition to receipt of the award, an acknowledgement that such awards, as well as any previously awarded compensation that falls within the scope of the Clawback Rules, will be subject to the Clawback Rules (carefully specifying whether and to what extent such compensation will also be within the scope of any supplemental clawback policy company has in effect) and allowing for broad recovery and offset rights in favor of the company. In conducting these reviews, companies should be mindful that significant questions remain as to how to reconcile potential tensions between the Clawback Rules and other applicable laws, including state and local laws that broadly protect "wages" against forfeiture or clawback and limitations in the tax rules for recovery of taxes paid on amounts that are ultimately clawed back. While the Clawback Rules contain limited impracticablity exemptions which include violations of the company's home country law, the SEC has indicated that inconsistency between its rules and any existing compensation contracts would not be an excuse for failure to recover and noted that companies have had ample notice of the statutory mandate for the SEC's adoption of the Clawback Rules. A careful review is especially important after a recent case involving the enforcement of a clawback policy emphasized that in addition to having a policy in place, companies would need to follow general principles regarding the enforceability of contracts in order in to claw back compensation, such that ensuring executives sign an acknowledgement as described above is advisable.[6]

— Compensation committees may wish to consider the impact of the Clawback Rules on compensation plan design. We expect many compensation committees to work with their compensation consultants and advisors in structuring or modifying compensation programs with an eye toward enforcement of the Clawback Rules and potential mitigation of the effect of new clawback policies on executives' compensation. Potential considerations for modification may include:

- Using operational, strategic, or ESG measures as opposed to financial performance measures and/or moving away from a reliance on stock price or TSR as a financial performance measure given the difficulty in determining the impact of a restatement on incentive compensation earned based on the achievement of such metrics.

- Moving from awards with multiple year performance periods to incentive compensation that contains a "banking" element (*e.g.*, awards where performance is measured at one-year performance periods subject to continued employment through the end of the aggregate number of performance periods) to limit the scope of the award that may be covered by the company's clawback policy if a lookback period encompasses only a portion of the performance period.

- Implementing "plateau" performance metrics where a range of outcomes, as opposed to one point of achievement, may result in the same payout. For example, an annual performance bonus program where attainment of revenues in the range from $X to $Y result in 100% target payout. This sort of structure could minimize the impact of "little r" restatements on incentive-based compensation payouts given the general expectation that "little r" restatements are not likely to create drastic changes in relevant performance payout calculations.

- Requiring deferral of earned incentive compensation through the date it is no longer covered by the lookback period mandated by the Clawback Rules, longer stock ownership periods following settlement of equity awards, or similar steps to extend the period of time before earned incentive compensation becomes payable to covered executives in order to facilitate recovery.

The desire and ability of compensation committees to make any changes to plan design may be limited by countervailing interests of shareholders and proxy advisory firms.

Notably, however, the desire and ability of compensation committees to make any such changes to plan design may be limited by countervailing interests of shareholders and proxy advisory firms.

Indemnification

— The Clawback Rules generally prohibit a company from indemnifying or otherwise economically protecting executive officers from the Clawback Rules. Affected companies may wish to review their executive employment agreements and plans, as well

[6] *See* Hertz Corp. v. Frissora, 2:19-cv-08927, 2023 U.S. Dist. LEXIS 109846 (D.N.J. June 26, 2023). We note that the case is an unpublished federal district court opinion and would not be binding on companies. However, while the case does not create a binding precedent, it is possible that other courts will follow this approach and it gives a view as to how a judge may rule when it comes to the enforceability of a clawback policy.

as indemnification policies, to ensure compliance with this aspect of the rules.

Advisory Firm Guidelines

— We recommend monitoring institutional shareholder and proxy advisory firm policies for their guidelines regarding clawbacks. In revising its 2024 guidelines, Glass Lewis explained that in addition to meeting the requirements of the Clawback Rules, clawback policies should also provide companies with the power to clawback incentive compensation from an executive "when there is evidence of problematic decisions or actions, such as material misconduct, a material reputational failure, material risk management failure, or a material operational failure," regardless of whether the executive is terminated for cause.[7]

New Disclosure Requirement for Option/SAR Awards

On December 14, 2022, the SEC adopted new disclosure requirements under Regulation S-K requiring disclosure of a company's policies and practices on the timing of option and stock appreciation right (SAR) awards as well as certain tabular disclosure of awards of options and SARs to NEOs that occur close in time to the company's disclosure of material nonpublic information (MNPI). Companies are required to comply with new Item 402(x) of Regulation S-K (Item 402(x)) in the annual report that covers the first full fiscal year beginning on or after April 1, 2023, which for calendar year-end companies will cover option and SAR grants made to NEOs in fiscal 2024.

Required Disclosure

— **Narrative Disclosure** – Item 402(x) will require companies to discuss their policies and practices as to the timing of awards of options and SARs, as well as any other option-like awards, in relation to the disclosure of MNPI. The disclosure must include (1) how the company's board of directors determines when to grant such awards; (2) whether the company takes MNPI into account when determining the timing of an award, and if so, how; and (3) whether the company has timed the disclosure of MNPI to affect the value of executive compensation. Companies are required to include this narrative disclosure regarding their policies and practices regardless of whether the company has actually made grants of option-like awards close in time to the release of MNPI. This disclosure is not required for full-value awards like restricted stock or restricted stock units.

— **Tabular Disclosure** – If the company has awarded options or SARs to a NEO within the period starting four business days before filing a periodic or current report (other than an 8-K disclosing a new option award pursuant to Item 5.02(e) of Form 8-K) that discloses MNPI and ending one business day after such filing, the following disclosure is required in a tabular format: (1) the name of the NEO; (2) the grant date of the award; (3) the number of securities underlying the award; (4) the per-share exercise price; (5) the grant date fair value of the award; and (6) the percentage change in the closing market price of the underlying securities between the trading day ending immediately prior to the disclosure of MNPI and the trading day beginning immediately following the disclosure of MNPI.

Next Steps

— **Adopt or Update a Formal Grant Policy** – Companies should plan to adopt a formal grant policy if one is not already in place or update their existing policy to mitigate the likelihood of triggering the tabular disclosure set forth in the new rule. Companies may choose to implement a grant policy that sets a fixed schedule for the granting of routine option and SAR awards to occur in an open trading window shortly after the release of MNPI but retain flexibility to deviate from this schedule as needed for off-cycle grants (*i.e.*, for new hires or in connection with acquisitions).

[7] Glass Lewis, *supra note 3*.

— **Update Equity Grant Disclosure in CD&A** – Companies should review their existing disclosure related to their equity award grant practices in the Compensation Discussion & Analysis section of their proxy and consider any necessary updates to comply with the new requirements as it relates to option and SAR award grant practices and to reflect any changes to their current grant policies implemented as a result of the new rule.

Sustainability Reporting

Amélie Champsaur
Partner
Paris
achampsaur@cgsh.com

Camille Kernevès
Associate
Paris
ckerneves@cgsh.com

Andreas Wildner
Associate
London
awildner@cgsh.com

EU Corporate Sustainability Reporting Directive

After several years during which the EU's Corporate Sustainability Reporting Directive (CSRD) had been hotly discussed and anticipated, 2023 saw not only the entry into force of the CSRD itself,[1] but also the adoption and publication of the European Sustainability Reporting Standards (the ESRS).[2]

2024 marks the start of the phase-in of the new reporting requirements, with the first CSRD compliant reports being required to be published by large EU-based "public-interest entities" in respect of financial years starting on or after 1 January 2024 (see chart on the next page).

Groups that may be subject to CSRD should therefore carry out a mapping exercise to determine which EU and non-EU companies are in scope and the timing and manner in which they will comply with the disclosure requirements (e.g. at entity level, sub-consolidated level or consolidated group level).

International trends

While the CSRD's requirements stand out from the landscape of international reporting requirements – not least because the broad scope of sustainability matters to be reported, the EU's "double materiality" perspective, and the mandatory disclosure of Paris-Agreement-aligned transition plans – there are a number

[1] Official Journal of the European Union, "Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 amending Regulation (EU) No 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU, as regards corporate sustainability reporting" (December 16, 2022), available here.

[2] Official Journal of the European Union, "Commission Delegated Regulation (EU) 2023/2772 of 31 July 2023 supplementing Directive 2013/34/EU of the European Parliament and of the Council as regards sustainability reporting standards" (December 22, 2023), available here.

Phase-in timeline	
Date of application	**Type of reporting entity**
from 2025 (2024 FY reports)	Large EU "public-interest entities" and large issuers of EU-listed securities (under the NFRD thresholds)
from 2026 (2025 FY reports)	• Other large EU companies, including large subsidiaries of third country groups (under the CSRD thresholds); and • Large issuers of EU-listed securities (under the CSRD thresholds)
from 2027 (2026 FY reports)	SMEs listed on EU regulated markets (except micro-undertakings)
from 2029 (2028 FY reports)	Third country groups with an EU turnover >150M€ and a large subsidiary or branch in the EU

of international developments that Boards should continue to monitor.

One of these is the international regulatory uptake of the International Sustainability Standards Board's (ISSB's) IFRS S1 and IFRS S2 standards,[3] published in June last year. The UK, for example, has already confirmed its intention to base its future sustainability disclosure standards on the ISSB framework.[4] 2024 will also likely see the finalisation of the US Securities and Exchange Commission's climate disclosure rules.

Another trend to watch is the increasing focus on nature- and biodiversity-related disclosures. In September 2023, the Taskforce on Nature-related Financial Disclosures published its disclosure recommendations,[5] and it is expected that this topic will assume increasing importance over this year in the minds of both standard-setters such as the ISSB as well as regulators.

[3] For additional information on IFRS, see our July 2023 alert memo available here.

[4] U.K. Department for Business and Trade, "UK Sustainability Disclosure Standards" (August 2, 2023), available here; U.K. Financial Conduct Authority, "Primary Market Bulletin 45" (August 10, 2023), available here.

[5] Taskforce on Nature-related Financial Disclosures, "Recommendations of the Taskforce on Nature-related Financial Disclosures" (September 2023), available here.

EU Taxonomy

The EU Taxonomy Regulation[6] provides a framework definition of environmentally sustainable economic activities to promote sustainable investment and combat greenwashing. Subsequent implementing acts set sector-specific sustainability criteria for a number of "high impact" activities that are considered key to the green transition, and specify the content and presentation of information to be disclosed on environmentally sustainable economic activities, as well as the methodology to comply with this disclosure obligation.

For the purposes of the EU Taxonomy Regulation, an economic activity is considered to be environmentally sustainable or "aligned" if it meets all of the following requirements:

— It substantially contributes to one or more of the six environmental objectives of the EU Taxonomy Regulation in accordance with certain technical standards: (i) climate change mitigation; (ii) climate change adaptation; (iii) sustainable use and protection of water and marine resources; (iv) transition to a circular economy; (v) pollution prevention

[6] Official Journal of the European Union, "Regulation (EU) 2020/852 of the European Parliament and of the Council of 18 June 2020 on the establishment of a framework to facilitate sustainable investment, and amending Regulation (EU) 2019/2088" (the "EU Taxonomy Regulation") (June 22, 2020), available here.

Gradually, more EU companies will be required to comply with the EU Taxonomy Regulation requirements, in line with the phased approach of the CSRD.

and control; and (vi) protection and restoration of biodiversity and ecosystems;

- It does not significantly harm any of the other environmental objectives; and
- It is carried out in compliance with certain minimum safeguards.

For the first two objectives, climate change mitigation and climate change adaptation, non-financial undertakings[7] were required to disclose their Taxonomy-alignment for the first time in 2023. Financial undertakings[8] will be required to disclose that Taxonomy-alignment from 2024. Gradually, more EU companies will be required to comply with the EU Taxonomy Regulation requirements, in line with the phased approach of the CSRD.[9]

In June 2023, the European Commission adopted:

- The Amended EU Taxonomy Climate Delegated Act[10] to broaden the scope of economic activities that contribute to climate change mitigation and adaptation (i.e. the first two objectives), including in the manufacturing and transportation sectors; and
- The EU Taxonomy Environmental Delegated Act[11], which establishes a new set of EU Taxonomy criteria for economic activities that make a substantial contribution to the four remaining objectives.

Beginning January 1, 2024, in scope companies will be required to disclose their percentage of Taxonomy-eligible activities with respect to these new criteria and activities. Disclosure of Taxonomy-alignment in line with theses delegated acts will be required from 2025 for non-financial undertakings and from 2026 for financial undertakings.

Similar to CSRD, companies should be monitoring the Taxonomy regulations to determine if and when their activities may be reportable.

Mandatory Sustainability Due Diligence

On February 23, 2022, the European Commission published a legislative proposal for a Directive on Corporate Sustainability Due Diligence (“CS3D”),[12] aimed at promoting sustainable and responsible corporate behavior and integrating human rights and environmental considerations into companies’ operations and corporate governance.

As a result of inter-institutional negotiations, the European Parliament and the Council reached a provisional agreement on December 14, 2023. The provisional agreement must now be approved and formally adopted by both institutions before it can enter into force.

7 A non-financial undertaking is an undertaking that is subject to the disclosure obligations laid down in Articles 19a and 29a of the Accounting Directive and is not a financial undertaking (Article 1(9) of the Disclosures Delegated Act).

8 A financial undertaking is an undertaking that is subject to the disclosure obligations laid down in Articles 19a and 29a of the Accounting Directive and is an asset manager, a credit institution, an investment firm, an insurance undertaking or a reinsurance undertaking (Article 1(8) of the Disclosures Delegated Act).

9 The EU Taxonomy Regulation applies inter alia to “*undertakings which are subject to the obligation to publish a non-financial statement or a consolidated non-financial statement pursuant to Article 19a or Article 29a of the Accounting Directive, respectively*” (Article 1(c)). As such, the entry into force of the CSRD has an impact on the scope of application of the EU Taxonomy Regulation.

10 Official Journal of the European Union, “Commission Delegated Regulation (EU) 2023/2485 of 27 June 2023 amending Delegated Regulation (EU) 2021/2139” (November 21, 2023), available here.

11 Official Journal of the European Union, “Commission Delegated Regulation (EU) 2023/2486 of 27 June 2023” (November 21, 2023), available here.

12 European Commission, “Proposal for a Directive on corporate sustainability due diligence and annex” (February 23, 2022), available here.

Under the provisional agreement,[13] companies will have to, among other things:

- Integrate due diligence into their policies and risk management systems;
- Adopt a plan to ensure that their business model complies with limiting global warming to 1.5°C;
- Identify, assess, prevent, mitigate, end and remedy their negative impacts and those of their upstream and downstream partners;
- Engage meaningfully with those affected by their actions;
- Establish a complaints mechanism;
- Communicate on their due diligence policies; and
- Monitor the effectiveness of their due diligence policies and measures on a regular basis.

The CS3D will apply to EU companies with more than 500 employees and a net worldwide turnover more than €150 million, non-EU companies with a turnover generated in the EU of more than €150 million, and to smaller EU and non-EU companies in high-risk sectors such as the manufacture of textiles, clothing and footwear, agriculture, mineral resources and construction. Financial services will initially be excluded from the scope of the CS3D, but there will be a review clause for a possible future inclusion.

Each EU Member State will designate a supervisory authority to monitor firms' compliance with the due diligence requirements and will have the power to conduct inspections and investigations and to impose sanctions on non-compliant firms, including "naming and shaming" and fines of up to 5% of their worldwide net turnover.

Civil liability will also be available to victims of companies that fail to meet their due diligence obligations.

The CS3D is expected to be adopted in early 2024, with a two-year period from the date of entry into force for Member States to implement it into national law, so the CS3D is not expected to apply to the first in-scope entities before 2026.

It is likely, however, that over the course of 2024, efforts to tackle greenwashing will increase, as a result of legislative efforts as well as litigation.

Greenwashing – Turning up the Heat

A topic that should be considered carefully by Boards in 2024 is greenwashing.

So far, much of the focus in respect of greenwashing has been on regulators' trying to formulate clear expectations for businesses within their regulatory remit. For example, in June last year, the European Supervisory Authorities (ESMA, EBA, EIOPA) published progress reports on greenwashing, setting out their current thinking on greenwashing and related risks in their respective sectors.[14]

It is likely, however, that over the course of 2024, efforts to tackle greenwashing will increase, as a result of legislative efforts as well as litigation.

[13] European Parliament News, "Corporate due diligence rules agreed to safeguard human rights and environment" (December 14, 2023), available here; European Council of the European Union, "Corporate sustainability due diligence: Council and Parliament strike deal to protect environment and human rights" (December 14, 2023), available here.

[14] European Securities and Markets Authority, "Progress Report on Greenwashing" (May 31, 2023), available here; European Banking Authority, "EBA Progress Report on Greenwashing Monitoring and Supervision" (May 31, 2023), available here; European Insurance and Occupational Pensions Authority, "EIOPA Advice to the European Commission on Greenwashing" (June 1, 2023), available here.

The European Commission has already proposed (i) amendments to the Unfair Commercial Practices Directive and the Consumer Rights Directive with the aim of "empowering consumers for the green transition through better protection against unfair practices and better information";[15] and (ii) a new Directive on substantiation and communication of explicit environmental claims.[16] Both instruments are expected to be adopted in the course of 2024. Greenwashing risk, particularly in respect of past statements, is also heightened by increasing disclosure requirements (*e.g.*, those imposed by the CSRD).

Independently from these legislative developments, 2023 has already seen a drastic increase in greenwashing litigation and other enforcement action making it into the headlines. Actions have been brought in Europe, for example in the Netherlands,[17] and a claim challenging the validity of carbon-credit based carbon-neutrality claims was upheld in the Düsseldorf Regional Court in Germany.[18] That greenwashing claims can, in principle, give rise to civil liability in courts was shown several years ago by the class action brought by Altroconsumo against VW before the Court of Venice.[19] In France, the case against TotalEnergies for greenwashing based on misleading commercial practices under the French Consumer Code is progressing on the merits, as the Paris Judicial Court ruled in May 2023 that the three NGOs (Greenpeace France, Amis de la Terre France and Notre Affaire à Tous) had standing to bring their case.[20]

Other Regulatory Developments

In addition to the above developments, Boards should be aware of the vast range of other ESG-related regulatory developments in the EU. A few highlights:

— Towards the end of 2024, the majority of the EU's new Regulation on deforestation-free products[21] will begin to apply;

— 2024 may see the adoption of the EU's proposed forced labor ban;[22]

— A number of key initiatives under the EU's Circular Economy Action Plan are expected to progress significantly. Amongst other things, the overhaul of the EU's eco-design framework (including the introduction of a new digital product passport) is expected for 2024;[23] in the batteries space, not only will the majority of requirements under the new Batteries Regulation[24] begin to apply, but the proposed Critical Raw Materials Act[25] will likely be adopted and the Commission has also announced that it would set up a EUR 3 billion fund to support

15 European Commission, "Proposal for a Directive of the European Parliament and of the Council amending Directives 2005/29/EC and 2011/83/EU as regards empowering consumers for the green transition through better protection against unfair practices and better information" (March 30, 2022), available here; the European Parliament and the Council of the European Union reached a political agreement on October 25, 2023, available here.

16 European Commission, "Proposal for a Directive of the European Parliament and of the council on substantiation and communication of explicit environmental claims (Green Claims Directive)" (March 22, 2023), available here.

17 Sabin Center for Climate Change Law, "FossielVrij NL v. KLM" (2022), available here.

18 Sabin Center for Climate Change Law, "Deutsche Umwelthilfe v. TotalEnergies Warme & Kraftstoff Deutschland GmbH" (2022), available here.

19 Sabin Center for Climate Change Law, "Altroconsumo v. Volkswagen Aktiengesellschaft and Volkswagen Group Group Italia S.p.A." (2016), available here.

20 Greenpeace France, "Assignation Devant Le Tribunal Judiciaire de Paris" (March 2, 2022), available here (in French language) and here (unofficial English translation).

21 Official Journal of the European Union, "Regulation 2023/1115 of the European Parliament and of the Council of 31 May 2023" (June 9, 2023), available here.

22 The Commission proposal for a regulation prohibiting products made with forced labour on the Union market is accessible here.

23 European Commission, "Proposal for a Regulation of the European Parliament and of the Council establishing a framework for setting ecodesign requirement for sustainable products and repealing Directive 2009/125/EC" (March 30, 2022), available here.

24 Official Journal of the European Union, "Regulation 2023/1542 of the European Parliament and of the Council of 12 July 2023" (July 28, 2023), available here.

25 European Commission, "Proposal for a Regulation of the European Parliament and of the Council establishing a framework for ensuring a secure and sustainable supply of critical raw materials and amending Regulations (EU) 168/2013, (EU) 2018/858, (EU) 2018/858, 2018/1724, and (EU) 2019/1020" (March 16, 2023), available here. For an analysis of the proposed regulation, see our firm's dedicated alert memo, accessible here.

the European batteries industry.[26] Other important initiatives to monitor relate to the proposed "right to repair" as well as the new requirements applicable to packaging and packaging waste, which could have impacts across a broad range of industries;

— Lastly, 2024 will likely see the creation of a new framework for the regulation of ESG ratings.[27]

The Duty of Vigilance Law anticipates in many respects on the CSRD and CS3D and litigation under this law could offer a preview of possible actions under these EU frameworks.

Litigation – Some highlights

France

Duty of Vigilance Law

Pursuant to France's "Duty of Vigilance Law", adopted in 2017, a company may be given a formal notice to publish a vigilance plan in accordance with the Duty of Vigilance Law, which should explain what measures the company has implemented to identify and prevent human rights and environmental violations associated with the company's activities. If the company does not comply with the formal notice within a period of three months, the competent court (or the president of the court acting in summary proceedings) may, at the request of any person justifying an interest, order the company to comply with such obligations and may impose penalty payments for this purpose.

The Duty of Vigilance Law anticipates in many respects on the CSRD and CS3D and litigation under this law could offer a preview of possible actions under these EU frameworks.

In 2023, the Paris Judicial Court issued its first decision on the merits in a case involving the La Poste Group. The Paris Judicial Court ordered La Poste Group to: (i) complete its vigilance plan with a risk map identifying and prioritizing risks; (ii) establish procedures to assess subcontractors based on specific risks identified in the risk map; (iii) supplement its vigilance plan with a mechanism for alerting and collecting reports after consulting representative unions; and (iv) adopt and publish measures for the monitoring vigilance measures. This decision could pave the way for similar decisions in the future.

Given the number of pending cases,[28] other decisions are expected in 2024 that will likely further clarify the scope of the duty of vigilance for companies pending the adoption and subsequent implementation of the CS3D into national law.

[26] European Commission, "Commission proposes one-off extension of the current rules of origin for electric vehicles and batteries under the Trade and Cooperation Agreement with the UK" (December 6, 2023), available here; European Commission, "Proposal for a Council Decision as regards the transitional product-specific rules for electric accumulators and electrified vehicles" (December 6, 2023), available here.

[27] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on the transparency and integrity of Environmental, Social, and Governance (ESG) rating activities" (June 13, 2023), available here. For an analysis of the proposed regulation, see our June 2023 alert memo, available here.

[28] According to publicly available information, the cases currently pending before Paris Judicial Court or Paris Court of Appeal include the following:
- TotalEnergies (greenhouse gas emissions; protection of people and the environment in the context of oil projects in Uganda and Tanzania);
- EDF (respect of indigenous peoples' rights in the context of a wind farm project in Mexico);
- Rocher Group in relation to (freedom to join a union and discriminations against women with respect to a Turk subsidiary);
- Suez (right to water in Chile);
- Casino (deforestation, indigenous' rights abuses and forced labor in Brazil and Colombia);
- Danone (inadequate acknowledgement and management of plastic pollution).

Criminal complaints

In 2023, far-reaching criminal complaints were filed in connection with the protection of the environment. By way of example, on September 22, 2023, four NGOs sued TotalEnergies for four alleged criminal offences: abstention from fighting a disaster, involuntary manslaughter, involuntary personal injury, and destruction or damage to the property of others likely to cause danger to persons. While TotalEnergies has denied these allegations, the NGOs seek to demonstrate that TotalEnergies had the opportunity to take action to combat climate change by limiting its investments in the fossil fuel sector, but instead continued to develop new oil and gas infrastructure, thereby contributing to the aggravation of a crisis that endangers a large part of the world's population.

Germany

German Supply Chain Due Diligence Act

On 1 January 2023 the German Supply Chain Act (Lieferkettensorgfaltspflichtengesetz) came into effect. While the Act initially applied to German-based companies with more than 3,000 employees, since 1 January 2024, Companies with more than 1,000 employees per average per fiscal year in Germany (including in affiliated companies) came into scope. The Act will likely be amended when the EU introduces CS3D.

The Act imposes on German companies[29] extensive due diligence compliance obligations with regard to human rights and environmental protection along the supply chain. More specifically, in-scope companies are required to adopt certain policies and processes related to supply chain due diligence (including in respect of risks connected to indirect suppliers), implement preventative measures and complaint procedures, conduct risk analyses, provide remedial action in the event of a human rights violation, document and report on the fulfilment of its due diligence obligations, and review the efficacy of their policies and processes at least annually as well as on an ad hoc basis. Notably, the Act establishes a duty of effort, but not an obligation of result. As such, in-scope companies must prove they have done everything they can to prevent human rights-related risks along the supply chain under the "principle of adequacy", resulting in the obligation for the companies to use reasonable best efforts.

The Federal Office of Economics and Export Control ("Bundesamt für Wirtschaft und Ausfuhrkontrolle" or BAFA) is responsible for monitoring and enforcing the Supply Chain Act. In 2023, approximately 40 complaints in total were filed with BAFA under the Act. Reportedly, only in six cases did BAFA actually contact the relevant companies, and it has not, so far, imposed any sanctions under the Act. While BAFA itself does not provide information about specific cases, it has further been reported that NGOs filed complaints against German food retailer Edeka and Rewe for alleged breaches of the Act.[30] Further complaints were filed by trade unions and NGOs: one against Tom Tailor, Amazon and IKEA in April 2023[31] for allegedly failing to adequately monitor conditions in their factories and endangering the safety of workers; and another against Volkswagen, BMW and Mercedes-Benz in June 2023[32] for alleged human rights violations in their supply chains in the Xinjiang Uygur Autonomous Region.

Litigation in relation to the German Climate Protection Act

The 2021 Neubauer et al. v. Germany ruling[33] by the German Constitutional Court led to a review of the German Climate Protection Act, as some parts of

[29] Companies regardless of legal form having their head office, principal place of business, administrative headquarters, statutory registered office or branch office in Germany.

[30] Spiegel Economy, "Oxfam files complaint against Edeka and Rewe" (November 3, 2023), available here.

[31] Due Diligence Design, "First case filed under the German Supply Chain Due Diligence Act against Tom Tailor, Amazon, and IKEA by Bangladeshi workers" (April 27, 2023), available here.

[32] Due Diligence Design, "Second case filed under the German Supply Chain Due Diligence Act" (July 6, 2023), available here.

[33] Climate Case Chart, "In the proceedings on the constitutional complaints of individuals from Germany against the failure of the Federal Republic of Germany to adopt suitable statutory provisions and measures to tackle climate change" (March 24, 2021), available here.

it were not in line with the targets set for reducing greenhouse gas emissions by 2030. The ruling also led to a significant increase in the number of civil cases brought by NGOs and individuals seeking to force polluting companies to change their climate-related policies and use of internal combustion engines. Since then, car manufacturers in particular have been sued for their impact on climate change, including Volkswagen,[34] Mercedes-Benz[35] and BMW.[36] However, a number of these cases were dismissed in 2022 and 2023 by German courts, which found that the companies either complied with their regulatory obligations or that there was insufficient evidence that the plaintiffs' individual rights were threatened.

UK

In the UK, a claim that, over 2023, was the focus of much attention in this area was ClientEarth's claim against Shell, which was based on the allegation that Shell's directors had failed to properly take into account the implications for the company of the economy's net-zero transition, and, thereby, had breached some of their directors' duties. The claim was ultimately unsuccessful.[37]

[34] Sabin Center for Climate Change Law, "Kaiser et al v. Volkswagen AG" (2021), available here; Sabin Center for Climate Change Law, "Allhoff-Cramer v. Volkswagen AG" (2021), available here.

[35] Sabin Center for Climate Change Law, "Deutsche Umwelthilfe (DUH) v. Mercedes- Benz AG" (2021), available here.

[36] Sabin Center for Climate Change Law, "Deutsche Umwelthilfe (DUH) v. Bayerische Motoren Werke AG (BMW)" (2021), available here.

[37] For additional information on the High Court reaffirming the decision against Shell's board, see our July 2023 alert memo available here; For additional information on Client Earth's order to pay Shell's costs after the dismissal of the derivative claim against Shell's board, see our September 2023 alert memo available here.

Voluntary Carbon Markets: Is It the CFTC's Time to Shine?

Deborah North
Partner
New York
dnorth@cgsh.com

Laura Daugherty
Associate
New York
ldaugherty@cgsh.com

Companies have identified that the voluntary carbon markets may play an important role in contributing to a reduction in their net greenhouse gas (GHG) emissions, and, therefore, in meeting their GHG emissions reduction goals. However, they have also exercised caution in embracing the voluntary carbon markets due to complicated standards, carbon credit quality issues and lack of market and pricing transparency.[1] Since 2020, the Commodity Futures Trading Commission (CFTC) has shown an increasing interest in regulating the voluntary carbon markets, and this interest has culminated in significant developments in 2023, including the Whistleblower Alert, establishment of its Environmental Fraud Task Force, the Second Voluntary Carbon Markets Convening and now the Proposed Guidance Regarding the Listing of Voluntary Carbon Credit Derivative Contracts. These CFTC initiatives have the potential to address some of the well-known challenges in the voluntary carbon markets, which may lead to a healthier and more robust market. We begin with a brief overview of the voluntary carbon markets before discussing the CFTC's recent actions in this area.

Voluntary Carbon Markets Overview

Voluntary carbon markets allow carbon emitters to purchase credits that are awarded to projects that remove or reduce atmospheric carbon. These credits offset the carbon emitters' own GHG emissions in furtherance of a voluntary commitment to reduce "net" emissions. Each credit typically corresponds to one metric ton of reduced, avoided or removed carbon dioxide or equivalent GHG.[2] Within the voluntary carbon markets, there are two main types of carbon credits:

— **avoidance credits**, which correspond to projects that prevent or reduce carbon emissions that would have otherwise occurred, such as renewable energy

1 *See* Dieter Holger, "Many Companies Are Shying Away From Carbon Credits" (January 17, 2023), available here.

2 *See* our January 2024 alert memo, available here, at 2.

projects, energy efficiency improvements and recycling projects; and

— **removal credits**, which correspond to projects that capture and store existing atmospheric carbon, such as afforestation, reforestation and implementation of carbon capture and storage technology.[3]

Not all carbon credits, however, are created equal, and differences in pricing reflect the market's faith in the "quality" of the specific carbon credit.

Not all carbon credits, however, are created equal, and differences in pricing reflect the market's faith in the "quality" of the specific carbon credit. For example, some believe that nature-based credits suffer from increased challenges because they may not offer permanence – e.g., there is always a risk that the trees that were planted as part of a project that generated the credits burn down – and this is often reflected in lower prices for these nature-based credits.

The voluntary carbon markets can be distinguished from "compliance" carbon markets, where a government or regulator issues a carbon allowance that participants must not exceed unless they can purchase additional compliance allowances from another participant under a cap-and-trade program.[4]

CFTC Action

In recent years, the CFTC has taken various, often compounding, actions to address fundamental issues in the voluntary carbon markets. The CFTC's focus on climate change and the voluntary carbon markets began in earnest in September 2020, when the CFTC's Climate-Related Market Risk Subcommittee issued a report titled Managing Climate Risk in the U.S. Financial System.[5] In response, in March 2021, then CFTC Acting Chairperson Rostin Behnam established the Climate Risk Unit.[6] In June 2022, the CFTC held its first Voluntary Carbon Markets Convening,[7] and, in concert, issued a Request for Information (RFI) on Climate-Related Financial Risk.[8] For more information regarding the CFTC's actions from 2020 through 2022, please see our January 2023 memo "Voluntary Carbon Markets: An Overview of U.S. Regulatory Developments," available here.

2023 saw acceleration of the CFTC's focus on the voluntary carbon markets. On June 20, 2023, the CFTC's Whistleblower Office in the Division of Enforcement issued an alert on how to identify and report potential Commodity Exchange Act (CEA) violations connected to fraud or manipulation in the carbon markets.[9] Shortly thereafter, on June 29, 2023, the CFTC announced it had established an Environmental Fraud Task Force. The purpose of the Task Force is to combat fraud and misconduct in regulated derivatives markets and relevant spot markets (such as voluntary carbon markets) relating to purported efforts to address climate change and other

3 *See* Grégoire Guirauden, "Avoidance and Removal Carbon Credits" (June 19, 2023), available here.

4 *See* our January 2024 alert memo, available here, at 2.

5 *See* Commodity Futures Trading Commission Press Release, "CFTC's Climate-Related Market Risk Subcommittee Releases Report" (September 9, 2020), available here; *see also* Rostin Behnam et al., "Managing Climate Risk in the U.S. Financial System: Report of the Climate-Related Market Risk Subcommittee, Market Risk Advisory Committee of the U.S. Commodity Futures Trading Commission" (2020), available here. We also note that in the Securities and Exchange Commission (SEC) and CFTC's joint 2012 product characterization final rule, the regulators discussed environmental commodities, such as emissions allowances, carbon offsets/credits or renewable energy certificates, that can be physically delivered and consumed as one example of intangible nonfinancial commodities that could underly a transaction subject to the forward contract exclusion from regulation as a swap. *See* Further Definition of ''Swap,'' ''Security-Based Swap,'' and ''Security-Based Swap Agreement''; Mixed Swaps; Security-Based Swap Agreement Recordkeeping, 77 Fed. Reg. 48208, 48233 (August 13, 2012).

6 *See* Commodity Futures Trading Commission Press Release, "CFTC Acting Chairman Behnam Establishes New Climate Risk Unit" (March 17, 2021), available here.

7 *See* Commodity Futures Trading Commission Press Release, "CFTC Announces Voluntary Carbon Markets Convening" (May 11, 2022), available here.

8 *See* Commodity Futures Trading Commission Press Release, "CFTC Releases Request for Information on Climate-Related Financial Risk" (June 2, 2022), available here.

9 *See* Commodity Futures Trading Commission Press Release, "CFTC Whistleblower Office Issues Alert Seeking Tips Relating to Carbon Markets Misconduct" (June 20, 2023), available here.

environmental risks.[10] On July 19, 2023, the CFTC held its Second Voluntary Carbon Markets Convening. The purpose of the Convening was to discuss current trends and developments in the cash and derivatives markets for carbon credits, public sector initiatives related to carbon markets, recent private sector initiatives for high quality carbon credits and market participants' perspectives on how the CFTC can promote integrity for high quality carbon credit derivatives.[11] The Convening confirmed that the CFTC intends to take a two-prong approach to its role in addressing potential fraud and manipulation in the voluntary carbon markets, exercising both: (i) its enforcement authority to prevent fraud and manipulation in the markets and (ii) its regulatory role to develop guidance relating to environmental products.[12]

Most recently, on December 4, 2023, the CFTC issued for public comment Proposed Guidance Regarding the Listing of Voluntary Carbon Credit Derivative Contracts. The Proposed Guidance acknowledges that participants in the voluntary carbon markets have faced challenges such as lack of standardization, transparency and integrity, and seeks to address these challenges through guidance issued to designated contract markets (DCMs)[13] over which the CFTC, as primary regulator, has clear authority.[14] In particular, the Proposed Guidance identifies certain factors that DCMs should address in the design of voluntary carbon credit derivatives contracts to avoid the possibility of manipulation. These factors include:

The CFTC intends to take a two-prong approach to its role in addressing potential fraud and manipulation in the voluntary carbon markets, exercising both: (i) its enforcement authority to prevent fraud and manipulation in the markets and (ii) its regulatory role to develop guidance relating to environmental products.

— **Quality Standards** such as (i) transparency, (ii) additionality, (iii) permanence and risk of reversal and (iv) robust quantification;

— **Delivery Points and Facilities**, taking into account the governance framework and tracking mechanisms of the crediting program underlying the VCCs, as well as the crediting program's measures to prevent double-counting; and

— **Inspection Provisions** or certification procedures for verifying compliance with the latest procedures in the voluntary carbon markets.[15]

Further, the Proposed Guidance places an affirmative obligation on DCMs to perform diligence on voluntary carbon credits underlying listed derivatives, and encourages DCMs to push crediting agencies towards robust quality standards, tracking mechanisms and internal governance in pursuit of heightened diligence standards, which, in turn, should foster market participant confidence in the contract and enhance liquidity.[16]

For more information on the Proposed Guidance, please see our December 2023 alert memo, available here, and January 2024 alert memo, available here. Comments on the CFTC's proposal are due on February 16, 2024.

[10] *See* Commodity Futures Trading Commission Press Release, "CFTC Division of Enforcement Creates Two New Task Forces" (June 29, 2023), available here.

[11] *See* Commodity Futures Trading Commission Press Release, "CFTC Announces Second Voluntary Carbon Markets Convening on July 19" (July 19, 2023), available here.

[12] For more information, *see* our July 2023 alert memo, available here.

[13] DCMs are CFTC-regulated exchanges that provide participants in the derivatives markets with the ability to execute or trade derivative contracts with one another. Commodity Futures Trading Commission, Commission Guidance Regarding the Listing of Voluntary Carbon Credit Derivative Contracts; Request for Comment, RIN 3038-AF40 (Dec. 4, 2023), available here ("Proposed Guidance") at 3 (citing 7 U.S.C. 1a(6)).

[14] *See* Proposed Guidance at 12-13.

[15] *See generally id.* at 23-37.

[16] *See generally id.* at 19-23.

Conclusion

Challenges with the voluntary carbon markets, such as complicated standards, carbon credit quality and integrity issues and lack of market transparency, have served as a barrier to entry for many companies, as well as a barrier to an efficient secondary market. But the voluntary carbon markets offer a promising alternative through which companies may offset their unavoidable emissions and therefore meet net GHG emissions goals. At COP28, the voluntary carbon markets were a main focus, and John Kerry, the U.S. climate envoy, said that the carbon markets may become "the largest marketplace the world will have ever known."[17]

The Proposed Guidance seeks to improve transparency regarding the quality of not only the voluntary carbon credit derivative contract, but also of the underlying GHG avoidance or removal project.

The CFTC is increasingly asserting its role in maintaining the integrity of the markets and thus fostering the market's potential for growth. We expect that the voluntary carbon markets will remain an area of focus for the CFTC, as the regulator seeks to shore up the markets against the possibility of manipulation and fraud. Notably, the Proposed Guidance seeks to improve transparency regarding the quality of not only the voluntary carbon credit derivative contract, but also of the underlying GHG avoidance or removal project. This increased transparency would provide companies with a way forward to conduct their own diligence regarding carbon credits, and would therefore help them to better assess both the carbon credits and the associates derivatives that they are trading in the markets. Boards of directors and executives, particularly those who have expressed skepticism regarding the reliability of the voluntary carbon markets, should monitor the CFTC's rulemaking and guidance in this area, as increased regulation may help to address some of the current shortcomings of the voluntary carbon markets and make those markets a more attractive source of achieving their environmental ambition. In the interim, boards of directors and executives should continue to look at how these markets evolve and whether they can support their companies' net zero commitments while keeping track of disclosure obligations as public filers.[18]

[17] Kenza Bryan, "COP28 Finance Leaders Try to Revive Decimated Carbon Credits Market" (December 5, 2023), available here.

[18] Notably, the SEC's climate rule is now on its Reg-Flex agenda for April 2024. *See* Securities and Exchange Commission, Agency Rule List – Fall 2023, available here. While a final climate rule has not yet been adopted, the proposed rule would require (i) mandatory disclosures by any registrant that maintains an internal carbon price regarding the price per metric ton of carbon dioxide, the total price and how it is estimated to change over time, the rationale for the internal carbon price, and how it uses the internal carbon price to evaluate and manage climate-related risks and (ii) any public filer who utilizes carbon offsets or renewable energy credits or certificates (RECs) as part of its net emissions reduction strategy to disclose the role of such carbon offsets or RECs in the registrant's climate-related business strategy, among other disclosure requirements. For additional information on the SEC's Climate Disclosures proposal, *see* our April 2022 alert memos available here; *see also* Securities and Exchange Commission, Proposed Rule: The Enhancement and Standardization of Climate-Related Disclosures for Investors, Securities Act Release No. 33-11042, Exchange Act Release No. 34-94478 (March 21, 2022), available here.

Generative AI Will Stay Top of Mind in 2024

Daniel Ilan
Partner
New York
dilan@cgsh.com

Marcela Robledo
Partner
Bay Area
mrobledo@cgsh.com

Lindsay Harris
Associate
New York
lharris@cgsh.com

Artificial Intelligence (AI), and in particular, generative AI, will continue to be an issue in the year to come, as new laws and regulations, agency guidance, continuing and additional litigation on AI and new AI-related partnerships will prompt headlines and require companies to continually think about these issues.

White House Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence[1]

On October 30, 2023, the Biden Administration issued a landmark Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (the Order), which sets forth the Administration's goals of establishing new or broadened standards for safety and security in the use of artificial intelligence and continuing to strengthen the foundation of protections with respect to Americans' privacy and civil rights, bolstering support for American workers, promoting responsible innovation, competition and collaboration and advancing America's role as a world leader with respect to AI.[2]

The Order tasks a number of federal departments and agencies with the responsibility of researching, generating, implementing and/or overseeing standards and guidance with respect to AI-related risks in their respective fields, generally through engaging in such agencies' proscribed rule-making procedures. Some instructions are specific and tailored to particular

---

1 Several states, such as New York and Connecticut, are also beginning to pass laws that address AI uses in their jurisdictions. These cover a variety of applications, such as criminal justice, employment, loans and education.

2 For additional details, see our November 2023 alert memo available here.

departments' activities, such as guidance offered to the Small Business Administration to consider prioritizing AI development and research through targeted allocation of grants and funding, and some directives are more general, such as where the Order calls on "relevant agencies" to establish guidelines and limitations on the appropriate use of generative AI and to provide personnel with access to secure and reliable generative AI capabilities.

In addition to the Order's enhancement of the pre-existing obligations imposed on federal agencies to oversee and implement responsible uses of AI (for example, clarifying the responsibility of regulated entities to conduct due diligence on and monitor any third-party AI services they use), the Order establishes a new White House AI Council, comprised of the heads of a number of federal agencies and executive offices, which will be responsible for coordinating the activities of the various federal agencies to ensure the effective formulation, development and communication, as well as timely implementation, of AI-related policies, while ensuring appropriate industry engagement.

The Order sets out myriad timelines for the various agencies to take action as instructed, ranging from 30 to 540 days following the Order, and some instructions have no timeline or are periodic (*e.g.,* annual reporting). It will be important to keep abreast of future rulemaking on this topic, in particular from the Federal Trade Commission and other agencies that have investigating powers over companies.

Next Steps for the Private Sector

At this phase, there are very few requirements in the Order that are applicable to private industry participants. The Order does establish a new reporting scheme for companies developing or planning to develop what the Order considers "dual-use foundation models," which are large-scale, widely adaptable models that can be used in a variety of contexts, and which demonstrate the ability to be used, or could be modified to be used, to threaten national security and economic stability (for example, by lowering the barrier to entry to develop chemical or nuclear weapons, or enabling powerful offensive cyber-attacks).

This change may create hiring opportunities for industry participants seeking to draw on AI talent from outside of the U.S. There are also funding opportunities centered around small businesses, education programs or employee development programs.

For private companies *without* dual-use foundation models, though, there are few applicable regulations coming out of this Order (that is, until agencies promulgate regulations in their respective fields that may apply to the private sector). However, there are several areas of potential opportunity for private AI companies to engage with these new policies. A key focus of the Order is drawing AI talent to the U.S. through recruiting programs, fast-tracked visas and interview procedures and focused immigration policies. This change may create hiring opportunities for industry participants seeking to draw on AI talent from outside of the U.S. There are also funding opportunities centered around small businesses, education programs or employee development programs. Beyond hiring and funding, there are also calls for increased government contracting, with the Order encouraging agencies to seek generative AI contracts with market players to optimize their own workforce and programs.

In addition to business opportunities, there are several opportunities for the industry to engage with regulators in the rulemaking process and provide comments. We encourage industry participants to be mindful and take advantage of the opportunity to provide industry insight for future regulation both from a commercial and technical standpoint.

U.S. Copyright Office and U.S. Patent Office Guidance on AI

In March 2023, the U.S. Copyright Office (USCO) launched an initiative geared towards examining copyright and intellectual property policy issues raised by AI—including both the scope of copyright protection for works generated using AI tools and the use of copyrighted materials to train AI. The initiative is the USCO's response to requests the Copyright Office has received from Congress and members of the public, including creators and AI users, to examine the issues raised in connection with copyright and AI.

Where the sole "author" of a work is an AI tool, such work will not be protectable under U.S. copyright laws.

One aspect of the initiative is new registration guidance, which imposes a duty on copyright owners to disclose AI-generated content in works submitted for copyright registration. The USCO has held in its guidance and in response to applications for copyright registration that human authorship remains a requirement in order for works of authorship to be eligible for copyright protection, and such position has been maintained by the federal courts. Where the sole "author" of a work is an AI tool, such work will not be protectable under U.S. copyright laws. The USCO's registration guidance, accessible on the USCO website,[3] includes instructions on how to disclose such AI-authored works, how to update any applications that are already pending and how to correct any already-approved applications to reflect the use of AI.

The U.S. Patent Office (USPTO) has also responded to the question of patentability of inventions created with the use of AI. The USPTO has determined, and federal courts have affirmed, that under U.S. patent laws, "inventorship" requires a natural person as the inventor, though the question of whether inventions created by humans with the assistance of AI may be eligible for patent protection has yet to be tested in the courts.

The USPTO recognizes that AI programs are becoming increasingly able to meaningfully contribute to innovation and has created a page of related guidance.[4] This guidance includes subject matter eligibility, disclosure requirements, examination guidance and functional limitations. The USPTO has also created a database of patented or applied-for patents that include AI technology.[5] Similar to the USCO, the USPTO has promulgated a series of trainings, both for inventors and examiners, as well as opportunities for industry participation from various stakeholders interested in shaping future guidance.

Ongoing AI-Related Litigation in the U.S.

The regulation of AI is still developing in the U.S.—unsurprisingly, at a slower pace than the technology itself, giving rise to a string of litigation as industry actors and stakeholders attempt to decipher how the development and deployment of AI technology intersects with intellectual property rights. The majority of lawsuits brought to date involve copyright infringement claims for the unauthorized use of copyrighted content to train AI models, including cases brought by authors for unauthorized use of their books (e.g., *Tremblay v. OpenAI, Silverman v. OpenAI*, *Kadrey v. Meta, Chabon v. OpenAI*, *Authors Guild v. OpenAI*, *Huckabee v. Meta, et al.* and *Sancton v. OpenAI*, to name a few), by artists for use of their artworks (e.g., *Andersen v. Stability AI, et al.*), or other content providers for use of their content (e.g., *Reuters v. ROSS*, *J.L. v. Alphabet*, *Doe v. GitHub*, *Concord Music Group v. Anthropic PBC* and *New York Times v. OpenAI*). Other claims include violations of publicity rights (*Young v. NeoCortext*), trademark and trade dress infringement (*Getty v. StabilityAI, Andersen v. Stability*), violation

3 *See* U.S. Copyright Office, "Copyright Office Launches New Artificial Intelligence Initiative" (March 16, 2023), available here.

4 *See* U.S. Patent and Trademark Office, "AI-related patent resources" (last updated May 27, 2022), available here.

5 *See* U.S. Patent and Trademark Office, "Artificial Intelligence Patent Dataset" (last updated December 29, 2022), available here.

of the Digital Millennium Copyright Act's provisions on copyright management information (CMI), unfair competition, unjust enrichment, violations of open-source licensing terms, breach of contract claims and others.

The court in Andersen dismissed the direct copyright infringement claims reiterating the importance of proving unauthorized reproduction, noting that mere usage by one AI model of or reliance on another already-trained model may not suffice for showing direct copyright infringement.

Many of these cases are still in early stages of litigation, but for some of them the courts have issued opinions, which continue to contour the legal landscape around these burgeoning issues. This is particularly true at the motion to dismiss stage, where we can see the level of variety in the pleadings and facts. The judge in *Reuters*, for example, issued an opinion at the summary judgment stage, denying both motions for summary judgment, reserving on the "fair use" analysis and finding that such issue needs to go to a jury. The court in *Andersen* dismissed all claims against two out of three defendants, reiterating the importance of proving unauthorized reproduction, noting that mere alleged usage by one AI model of or reliance on another already-trained model does not suffice for showing direct copyright infringement.[6] Similarly, the court in *Kadrey v. Meta* granted Meta's motion to dismiss in full, dismissing the claims that Meta's LLaMA model is itself an infringing derivative works for which Meta could be vicariously liable, that Meta violated the DMCA by omitting plaintiffs' CMI, and the unfair competition law, unjust enrichment and negligence claims. The court's order left intact only the claim for direct copyright infringement based on LLaMA's training (as to which Meta had not moved to dismiss), and plaintiffs ultimately opted not to amend their other claims and to proceed on the direct infringement claim alone. No court has yet reached the merits of the fair use defense, on which many of these cases are likely to turn.

The jurisprudence established through litigation and the forthcoming statutory regulation described above will continue to develop in tandem as the breadth of use-cases for AI technology continues to expand.

European Union Enacts an AI Act

On December 9, 2023, after a period of fraught negotiation, the European Parliament and Council reached a political agreement on the EU's Artificial Intelligence Act (AI Act).

The AI Act is likely to have a significant impact on the development, provision, distribution and deployment of AI systems in (and relating to) the EU, including (as was the case with the EU General Data Protection Act) as a result of extraterritorial aspects of the rules. It will therefore be of significant interest to boards of directors of companies headquartered outside the EU.

The AI Act proposes a risk-based approach to the regulation of artificial intelligence and machine learning systems (*i.e.,* with a sliding scale of regulatory requirements depending on the level of risk posed by use of such systems). Under this approach, the majority of AI systems are likely to fall into the category of minimal risk (*e.g.,* spam filters) and will not be covered by binding rules under the regulation. The bulk of the obligations (concerning both providers and deployers) under the AI Act will be imposed in respect of AI systems that are classified as high-risk. Further, a narrow set of AI system applications (*e.g.,* biometric categorization systems that use sensitive characteristics) will be prohibited outright.

Providers of certain types of popular consumer-facing AI systems (*e.g.,* chatbots) will be subject to specific transparency obligations, such as a requirement to make users aware that they are interacting with a machine. Deepfakes and other AI-generated content will also have to be labelled as such, and users will need to be

[6] For additional information, see our November 2023 blog post available here.

informed when biometric categorization or emotion recognition systems are being used. Additionally, providers will have to design systems in a way that ensures any synthetic audio, video, text, images or other content is marked in a machine-readable format, and detectable as artificially generated or manipulated.

As a next step, a consolidated final text will need to be prepared and formally approved by both the European Parliament and Council (which could happen as early as Q1 of 2024). As an EU regulation, the AI Act will be applied directly in the same way across all EU member states. Once it has entered into force, most of the general provisions of the AI Act will apply after a two-year grace period. Failure by companies to comply with the strictest provisions of the AI Act relating to prohibited AI systems may result in fines of up to €35 million or 7% of group global annual turnover (whichever is higher), while non-compliance with most other provisions of the AI Act (including rules relating to GPAI systems and models) may result in fines of up to €15 million or 3% of group global annual turnover (whichever is higher).

Regulatory enforcement actions underscore the importance of not deceiving consumers about the use of automated tools and how their data may be used to feed or train algorithms, and suggest that reliance on broad disclosures that PII is used to "develop or improve products and services" may be insufficient.

Developing and Updating Internal Policies and Procedures to Utilize and Implement AI Tools

With the growth of AI, a crucial next step for business entities is updating and/or developing internal company policies and procedures with respect to the use of AI. Companies utilizing AI tools should ensure they stay up to date with any legal developments that may impact such use, particularly with respect to data privacy and confidentiality, intellectual property rights, terms and conditions of use, reporting and record keeping, and should take care in updating and developing policies around AI.

Organizations that intend to use personally identifiable information (PII) in connection with AI tools should ensure that such usage has been appropriately disclosed to the relevant consumers at or before the time of collection in a privacy notice. Regulatory enforcement actions underscore the importance of not deceiving consumers about the use of automated tools and how their data may be used to feed or train algorithms, and suggest that reliance on broad disclosures that PII is used to "develop or improve products and services" may be insufficient. The consequences for unlawfully using PII in AI tools can be significant, as the FTC has required companies to delete not only unlawfully obtained data, but also the data products and algorithms developed using such data (known as algorithmic disgorgement).

Balancing business needs with implementing and maintaining transparent, ethical and responsible AI practices are the primary considerations in drafting an internal AI policy.

With respect to internal use of AI tools, for example by employees for internal business purposes, organizations should first determine whether they wish to encourage or discourage the use of AI on the job. Keeping with the Order discussed above, companies in highly regulated industries (*i.e.,* healthcare) or that directly impact other individuals (*i.e.,* credit reporting), may be inclined to restrict the use of AI for the time being, while others in less sensitive industries may seek to implement AI for business reasons (*i.e.,* potentially reducing operating costs). Balancing business needs with implementing and maintaining transparent, ethical and responsible AI practices are the primary considerations in drafting an internal AI policy.

Because the law around AI is developing daily, it may be difficult to ensure continued compliance without designating appropriate resources to stay abreast of the ever-evolving legal landscape. In addition to what has already been described arising out of the White House's Order on AI, in recent months, federal and state regulators have promulgated a vast array of guidance and legislation concerning implementation of AI tools in attempts to maintain pace with this rapidly growing technology. For example, the California Privacy Protection Agency recently released draft regulations (solely for discussion purposes) to outline a potential framework for PII usage in connection with automated decision making technologies. Under the current draft, entities would be required to provide consumers with "pre-use notices" describing how the business intends to use the consumer's PII for such technologies to allow the consumer to decide whether to proceed or opt-out, and whether to access more information. Further, the draft regulations also provide guidance on the scope of consumer opt-out requests, which would apply primarily in connection with decisions with potential to have significant impact on the consumer (*e.g.,* decisions about employment or compensation). Other regulators, such as the Colorado Attorney General, have also released binding regulations regarding the information required in connection with AI-specific data protection impact assessments.

Further, there are intellectual property and confidentiality risks to consider when drafting an internal corporate AI policy. As AI tools become more prevalent and widely adaptable, companies like Samsung and Amazon, as well as financial institutions including JPMorgan Chase, Bank of America and Goldman Sachs, have implemented controls and are drafting and revising policies addressing their institutions' internal use of ChatGPT and other similar AI tools amid growing concerns about potential privacy and regulatory risks.[7] Employees should be informed of the permitted (or prohibited) use and disclosure of proprietary or confidential business information and trade secrets in connection with their use of AI. To avoid missteps, in addition to guidance to employees, businesses should conduct diligence with respect to the confidentiality and use practices of any AI programs used by the business in order to confirm such programs implement proper safeguards with respect to any information shared with the AI tool. Further, in light of the current legal regime for IP protection of AI-generated works or inventions, when drafting internal AI policies, businesses should consider whether to allow employees to use AI to create or develop work product or inventions, depending on whether the business is reliant on IP protection (*i.e.,* copyright or patent protection) to safeguard such works. Companies choosing to develop AI models should set strict parameters around how and on what those models may be trained; instruct and monitor employees to ensure compliance; and maintain careful records to document the ethical sourcing, composition, filtering and use of training data. On the other hand, companies using third party AI models should minimize risk by carefully vetting the model selected and ensuring that their intended uses comport with the safety, ethics and privacy interests of their customers.

Companies seeking to train a model on data purchased from a vendor should also take care to look for appropriate representations and warranties as to the source of (and rights to) the data, as well as broad indemnification provisions should those representations prove unsound and lead to litigation.

[7] *See* Siladitya Ray, "Samsung Bans ChatGPT Among Employees After Sensitive Code Leak" (May 2, 2023), available here.

2023 Year-in-Review: Developments and Trends in White Collar Enforcement Litigation


Lisa Vicens
Partner
New York
evicens@cgsh.com


Matthew C. Solomon
Partner
Washington, D.C.
msolomon@cgsh.com


David A. Last
Partner
Washington, D.C.
dlast@cgsh.com


Andres Felipe Saenz
Senior Attorney
New York
asaenz@cgsh.com


Samuel Levander
Associate
New York
slevander@cgsh.com


Amira Perryman
Associate
New York
aperryman@cgsh.com

The Securities and Exchange Commission (SEC) and Department of Justice (DOJ) both accelerated their enforcement efforts in 2023, and seem poised to further intensify these efforts in 2024. At the same time, the SEC disseminated new disclosure requirements across sectors, including disclosures related to cybersecurity and artificial intelligence (AI), and renewed its focus on the corporate and social aspects of environmental, social and governance (ESG) guidance. Its Enforcement Division remained focused on litigating high-stakes cases in the digital assets space and expanded its sweep related to off-channel communications.

The DOJ has also charged several cases in the fraud and anti-money laundering space related to digital assets, including the recent trial conviction of Sam Bankman-Fried and the guilty pleas of Binance and its Chief Executive Officer, Changpeng Zhao. In addition, the DOJ made a number of announcements related to guidance and policies concerning corporate criminal enforcement, much of which is focused on fostering a culture of compliance within companies while continuing to pursue actions against alleged individual wrongdoers. The recent adoption of the Foreign Extortion Prevention Act (FEPA), companion legislation to the Foreign Corrupt Practices Act (FCPA), adds a new tool in the DOJ's arsenal to prosecute the recipients of foreign bribes, closing a notable gap and providing a mechanism to charge the "demand side" of foreign bribery. This new legislation is particularly timely as the DOJ continues to prioritize and remain active in its anti-corruption efforts involving both companies and individuals, including a number of significant FCPA matters in 2023.

SEC Enforcement Highlights

The SEC reported 784 total enforcement actions filed in 2023, a 3% uptick from the previous year, while total financial remedies dropped from $6.4 billion in 2022 to $4.9 billion in 2023.[1] The SEC continues to pursue aggressive enforcement actions against a variety of digital asset market participants, including issuers, trading and lending platforms and related individuals.[2] Like many of the investors it regulates, the SEC intensified its focus on AI in 2023, announcing a crackdown on AI disclosures and proposing a new rule governing AI-related conflicts of interest, with Chair Gary Gensler calling for cross-regulatory action to take on AI-related financial stability risks.[3] The SEC's whistleblower program also continued to grow: the SEC received over 18,000 whistleblower tips, topping last year's then-record of 12,300 tips, and distributed a record of almost $600 million in whistleblower awards, including a $279 million all-time-high award to one individual.[4] Finally, several settlements exemplified the SEC's continued focus on traditional areas of SEC oversight, including the regulatory activity of investment advisers, broker-dealers and credit rating agencies, compliance with Rule 206(4)-1 (the Marketing Rule),[5] and disclosure-related violations.[6]

The SEC continues to pursue aggressive enforcement actions against a variety of digital asset market participants, including issuers, trading and lending platforms and related individuals.

Digital Assets

Chair Gensler has made clear that he views the vast majority of digital asset industry participants as failing to comply with the securities laws. This position translated into lawsuits in federal court against several of the largest U.S.-based digital asset trading platforms for allegedly failing to register as securities exchanges, broker-dealers and clearing agents, all of which are premised on the SEC's allegations that dozens of digital assets sold and offered by these exchanges

1 Press Release, "SEC Announces Enforcement Results for FY23" (November 14, 2023), available here.

2 *See also* our November 2023 alert memo on this topic, "SEC Announces FY 2023 Enforcement Results with Second-Highest Penalties on Record", available here; Press Release, "SEC Charges NBA Hall of Famer Paul Pierce for Unlawfully Touting and Making Misleading Statements about Crypto Security" (February 17, 2023), available here; Press Release, "SEC Charges Kim Kardashian for Unlawfully Touting Crypto Security" (October 3, 2023), available here; Press Release, "SEC Charges Terraform and CEO Do Kwon with Defrauding Investors in Crypto Schemes" (February 16, 2023), available here; Press Release, "SEC Files 13 Charges Against Binance Entities and Founder Changpeng Zhao" (June 5, 2023), available here; Press Release, "SEC Charges Coinbase for Operating as an Unregistered Securities Exchange, Broker, and Clearing Agency" (June 6, 2023), available here; Press Release, "SEC Charges Samuel Bankman-Fried with Defrauding Investors in Crypto Asset Trading Platform FTX" (December 13, 2022), available here; Press Release, "SEC Charges LA-Based Media and Entertainment Co. Impact Theory for Unregistered Offering of NFTs" (August 28, 2023), available here.

3 Press Release, "SEC Proposes New Requirements to Address Risks to Investors from Conflicts of Interest Associated with the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers" (July 26, 2023), available here; Richard Vanderford, "SEC Head Warns Against 'AI Washing,' the High-Tech Version of 'Greenwashing'" The Wall Street Journal, (December 5, 2023), available here; Speech, "Remarks before the Financial Stability Oversight Council: 2023 Annual Report" (December 14, 2023), available here.

4 Press Release, "SEC Issues Largest-Ever Whistleblower Award" (May 5, 2023), available here.

5 *See also* our June 2023 alert memo on this topic, "SEC Expands the Scope of Its Marketing Rule Examination Sweep – But Still No Guidance", available here.

6 *See, e.g.,* Press Release, "SEC Announces Enforcement Results for FY23" (November 14, 2023), available here.

are securities.[7] However, the SEC has experienced mixed results in litigation in this space in 2023, with a summary judgment win against the digital asset issuer LBRY, a mixed decision on summary judgment against Terraform Labs where the court held that certain digital assets issued by Terraform Labs violated the securities laws while others did not, and a high-profile loss on summary judgment against Ripple, where the court held that the digital asset at issue (XRP) was not itself a security and Ripple did not engage in an unregistered securities offering when selling XRP on digital asset exchanges.[8] Following this decision, the SEC dismissed its sole claim against the current and former CEO of Ripple, representing a rare complete victory for individual defendants against the SEC in a high-profile litigated case.[9]

Early 2024 will present a series of critical tests for the SEC's digital asset agenda, with oral argument scheduled on defendants' motions to dismiss in two of the digital asset trading platform cases (Coinbase and Binance) in mid-January, and trial set to begin against Terraform Labs and its founder Do Kwon in late-January.

The SEC has continued to investigate and litigate cases regarding alleged internal controls weaknesses, increasing the number of actions based on alleged stand-alone controls violations without a separate violation of disclosure rules.

[7] In the complaints against two such platforms, Binance and Coinbase, the SEC alleged that 19 digital assets traded on these platforms were unregistered securities. *See* Complaint, *SEC v. Binance Holdings Limited*, No. 1:23-cv-01599 (D.D.C. June 5, 2023), available here; Complaint, *SEC v. Coinbase, Inc.*, No. 1:23-cv-04738, (S.D.N.Y. June 6, 2023), available here.

[8] Litigation Releases, "LBRY, Inc." (July 12, 2023), available here; *see also* Summary Judgment Order, *SEC v. Terraform Labs*, 1:23-cv-1346 (S.D.N.Y. December 28, 2023), available here; Summary Judgment Order, *SEC v. Ripple Labs, Inc.*, 1:20-cv-10832 (S.D.N.Y. July 13, 2023), available here.

[9] *See also* our News Listing on this topic, "Ripple CEO Brad Garlinghouse in Dismissal of All SEC Claims" (October 19, 2023), available here.

Internal Controls and Controls Disclosures

The SEC has continued to investigate and litigate cases regarding alleged internal controls weaknesses, increasing the number of actions based on alleged stand-alone controls violations without a separate violation of disclosure rules.[10] The SEC's key cases this year regarding public company financial reporting and disclosure failures included settlements with an advisory firm for its failure to adopt and implement adequate written policies to value assets in the funds managed by the firm,[11] with a leading financial news organization for alleged improper and misleading disclosures relating to its paid subscription service,[12] and with a transportation company and its former CEO for their failure to disclose perks provided to the former CEO and other executives.[13]

The SEC also finalized a rule that standardizes disclosure requirements related to cybersecurity incident reporting.[14] At the same time, the SEC has demonstrated its commitment to pursuing actions against companies that are victims of cyber-attacks. Most notably, the SEC charged a software company and its chief information security officer for fraud and internal control failures relating to allegedly known cybersecurity risks and vulnerabilities, alleging for the first time that a company's cybersecurity controls are part of the internal controls system required by the securities laws.[15]

[10] Press Release, "SEC Announces Enforcement Results for Fiscal Year 2023" (November 14, 2023), available here.

[11] Press Release, "SEC Charges Investment Adviser for Compliance Failures" (May 24, 2023), available here.

[12] Press Release, "SEC Charges Former MusclePharm Executives with Accounting and Disclosure Fraud" (June 27, 2023), available here; Press Release, "Bloomberg to Pay $5 Million for Misleading Disclosures About Its Valuation Methodologies for Fixed Income Securities" (January 23, 2023), available here.

[13] Press Release, "SEC Charges Global Transportation Company Greenbrier and Former CEO for Failing to Disclose Perks and Payments" (March 2, 2023), available here.

[14] Final Rule, "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure" (July 26, 2023) available here; Statement, "Cybersecurity Disclosure" (December 14, 2023), available here; *See also* Crossing a New Threshold for Material Cybersecurity Incident Reporting and our August 2023 alert memo on the SEC's cybersecurity disclosure rules available here.

[15] Press Release, "SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures" (October 30, 2023), available here; Complaint, *SEC v. SolarWinds Corp., 1:23-cv-09518 (S.D.N.Y. October 30, 2023), available* here.

Off-Channel Communications

The SEC's industry sweeps aimed at employees' alleged use of off-channel communications have continued, but at a slower pace than last year. In 2022, the SEC collected more than $1.2 billion in penalties from many of the largest financial institutions in the U.S. This year, the SEC filed settled actions against 25 broker-dealers, investment advisors and credit-rating agencies for a total additional $400 million in penalties.[16] As we enter the third year of this sweep, the SEC seems intent on further broadening the scope of its targets, as a variety of companies continue to agree to pay hefty fines even after voluntarily self-reporting their off-channel activity.[17]

ESG Enforcement

The SEC's enforcement priorities continue to include a focus on climate and ESG-related disclosure. In March 2023, the SEC agreed to a $55.9 million settlement of a litigated case against a mining company related to its safety disclosures in connection with a dam collapse, after voluntarily dismissing all intentional fraud claims against the company.[18] The SEC has also focused on enforcement actions related to the governance element of ESG, including a $35 million settlement with a video game company for allegedly failing to maintain disclosure controls and procedures to collect and analyze employee complaints of workplace misconduct, and charging, but because of substantial cooperation, declining to penalize, a fast food company in connection with its alleged failure to disclose the link between the departure of its CEO and allegedly improper workplace relationships.[19]

DOJ continues to focus on incentivizing voluntary self-disclosure through expanding the availability of declinations offered and increasing credit for cooperation and remediation, which results in discounts on penalties for corporations.

Key DOJ Developments

In 2023, the DOJ announced several policy updates and issued guidance in a number of areas related to corporate criminal enforcement and compliance. A steady theme of the announcements is that the DOJ continues to focus on incentivizing voluntary self-disclosure through expanding the availability of declinations offered and increasing credit for cooperation and remediation, which results in discounts on penalties for corporations.[20] Recent corporate resolutions demonstrate the DOJ's approach with respect to these new policies and guidance. The DOJ also remained focused on corporate enforcement across a variety of substantive areas, including FCPA, anti-money laundering, sanctions and digital assets, with conduct touching on various sectors and regions across the globe. Additionally, the

16 Press Release, "SEC Charges 10 Firms with Widespread Recordkeeping Failures" (September 29, 2023), available here.

17 Press Release, "SEC Charges 11 Wall Street Firms with Widespread Recordkeeping Failures" (August 8, 2023) available here (announcing penalties of $289 million against 11 firms for failing to maintain and preserve electronic records); Press Release, "SEC Charges 10 Firms with Widespread Recordkeeping Failures" (September 29, 2023), available here; Press Release, "SEC Charges HSBC and Scotia Capital with Widespread Recordkeeping Failures" (May 11, 2023), available here (announcing penalties of $15 million and $7.5 million against two firms for failing to maintain and preserve electronic communications).

18 Press Release, "Brazilian Mining Company to Pay $55.9 Million to Settle Charges Related to Misleading Disclosures Prior to Deadly Dam Collapse" (March 28, 2023), available here.

19 Press Release, "SEC Announces Enforcement Results for FY23" (November 14, 2023), available here; Press Release, "Activision Blizzard to Pay $35 Million for Failing to Maintain Disclosure Controls Related to Complaints of Workplace Misconduct and Violating Whistleblower Protection Rule" (February 3, 2023), available here; Press Release, "SEC Charges McDonald's Former CEO for Misrepresentations About His Termination" (Jan. 9, 2023), available here.

20 Speech, "Acting Assistant Attorney General Nicole M. Argentieri Delivers Remarks at the American Bar Association 10th Annual London White Collar Crime Institute" (October 10, 2023), available here; Speech, "Assistant Attorney General Kenneth A. Polite, Jr. Delivers Remarks on Revisions to the Criminal Division's Corporate Enforcement Policy" (January 17, 2023), available here; Press Release, "Albemarle To Pay Over $218M To Resolve Foreign Corrupt Practices Act Investigation" (September 29, 2023), available here; Press Release, "Corficolombiana to Pay $80M to Resolve Foreign Bribery Investigations" (August 10, 2023), available here.

DOJ continues to note its ongoing focus with respect to charging individuals alongside corporations.[21]

Policy Updates and Guidance

The DOJ issued policy updates and guidance focusing on encouraging and making clearer the benefits of self-reporting and cooperation; disciplining individual wrongdoers through clawing back compensation; updating compliance guidance, including with respect to off-channel communications; and providing a safe harbor for companies that detect, report and act to remediate misconduct at target companies in the M&A context.[22] These policies are:

— **Revised Corporate Enforcement Policy**:[23] This year saw significant modifications to the DOJ Criminal Division's Corporate Enforcement and Voluntary Self-Disclosure Policy (CEP). The previous policy had provided the presumption of a declination for a company that voluntarily self-disclosed, fully cooperated and appropriately remediated misconduct, but only where there were no "aggravating circumstances" present.[24] The revised CEP creates a specific path for a company to qualify for a declination notwithstanding the presence of aggravating circumstances, provided that the following heightened requirements are met: (i) the company made the voluntary self-disclosure immediately upon becoming aware of the allegation of misconduct, (ii) at the time of the misconduct and disclosure, the company had an effective compliance program and system of internal controls; and (iii) the company provided extraordinary cooperation to the DOJ and undertook extraordinary remediation.[25] In explaining "extraordinary," the DOJ has made clear that it is looking for something that goes "above and beyond" and is not simply "run of the mill" cooperation.[26] Under the revised policy, where the DOJ seeks a criminal resolution for a company that voluntarily self-discloses, it will provide cooperation credit between 50% to 75% off the bottom of the applicable U.S. Sentencing Guidelines range and will generally not require a corporate guilty plea, including for criminal recidivists. This is a significant jump from the prior 50% maximum credit available to cooperating companies and is consistent with the DOJ's broader message of providing "bigger carrots" to incentivize companies to self-report misconduct, while wielding a "bigger stick" for companies that do not.[27] Going forward, it remains to be seen how the DOJ will interpret what constitutes "timely" self-reporting and how that will affect cooperation credit. Additionally, under the revised CEP, companies that do not voluntarily self-disclose are nonetheless eligible for increased cooperation credit up to 50% off of the applicable U.S. Sentencing Guidelines range, instead of the previous maximum of 25% under the earlier policy.[28] The DOJ has explained

[21] Press Release, "Statement Of U.S. Attorney Damian Williams On The Conviction Of Samuel Bankman-Fried" (November 20, 2023) available here; Press Release, "Commodities Trading Company Agrees to Pay Over $98M to Resolve Foreign Bribery Case" (December 14, 2023), available here; Speech, "Acting Assistant Attorney General Nicole M. Argentieri Delivers Keynote Address at the 40th International Conference on the Foreign Corrupt Practices Act" (November 29, 2023), available here (discussing Corporate Enforcement Policy declination of Corsa Coal and charges against two former executives).

[22] The DOJ also updated its guidance on the selection of corporate compliance monitors. *See* DOJ, "Revised Memorandum on Selection of Monitors in Criminal Division Matters" (March 1, 2023), available here; Speech, "Assistant Attorney General Kenneth A. Polite, Jr. Delivers Keynote at the ABA's 38th Annual National Institute on White Collar Crime" (March 3, 2023), available here.

[23] DOJ, "Criminal Division Corporate Enforcement and Voluntary Self-Disclosure Policy" (updated January 2023) available here; *See, e.g.,* In re: Corsa Coal Corporation (CEP Declination Letter) (March 18, 2023), available here. In that matter, the DOJ issued a declination pursuant to the Criminal Division's Corporate Enforcement and Voluntary Self-Disclosure Policy and declined to prosecute Corsa Coal, a coal producer, for violations of the FCPA where certain company employees and agents were allegedly involved in a scheme to bribe foreign government officials in Egypt. The DOJ noted that it declined to prosecute based, in part, on the company's full and proactive cooperation with the DOJ's investigation and its timely and appropriate remediation. The company also agreed to disgorge its profits earned from the scheme, which was reduced to $1.2 million based on the company's inability to pay the full disgorgement amount.

[24] CEP declinations are also still subject to the disgorgement of ill-gotten gains. *See also* our January 2023 alert memo on this topic, "U.S. Department of Justice Announces Revisions to Corporate Criminal Enforcement Policy" , available here.

[25] The DOJ has explained that in determining what qualifies as "extraordinary" cooperation, it will look at indicia such as the immediacy and consistency of a company's cooperation, the degree to which a company cooperates with the DOJ, and the impact of that cooperation on the DOJ's own investigation. *See* Speech, "Assistant Attorney General Kenneth A. Polite, Jr. Delivers Remarks on Revisions to the Criminal Division's Corporate Enforcement Policy" (January 17, 2023), available here.

[26] *Id.*

[27] *See also* our January 2023 alert memo on this topic, "U.S. Department of Justice Announces Revisions to Corporate Criminal Enforcement Policy", available here.

[28] *Id.*

that in assessing cooperation credit, it will use the "full spectrum" of zero to 50% cooperation credit and that "every company starts with zero credit and must earn any benefit."[29]

The DOJ announced its intention to more closely consider compensation structures and consequence management when assessing the effectiveness of a company's compliance program.

— **Compensation Incentives and Clawback Pilot Program:**[30] In March 2023, Deputy Attorney General (DAG) Lisa Monaco announced that the DOJ wanted companies to ensure that employees are personally invested in promoting compliance by "having skin in the game" through compensation structures that create financial incentives and disciplinary measures, shifting the burden of corporate malfeasance onto those more directly responsible.[31] As part of those efforts, the DOJ announced its intention to more closely consider compensation structures and consequence management when assessing the effectiveness of a company's compliance program.[32] Under the DOJ's revised compliance guidance (known as the Evaluation of Corporate Compliance Programs), prosecutors will evaluate specific key metrics including (i) the transparency of a company's design and implementation of its compliance-promoting compensation system; (ii) the breadth of disciplinary actions—including compensation clawbacks—available to management to enforce compliance, and their consistent enforcement across different geographies and levels of the organization; and (iii) the tracking of relevant compliance-related metrics such as the percentage of compensation subject to cancellation or recoupment from those engaged in wrongdoing.[33] In addition, the DOJ Criminal Division announced the launch of a three-year Pilot Program Regarding Compensation Incentives and Clawbacks (the Pilot Program), which encourages companies to claw back compensation to punish employee misconduct and/or non-cooperation, and reward companies that implement compliance-related criteria in their compensation and bonus systems.[34] The Pilot Program requires companies entering into a resolution with the DOJ Criminal Division to implement compliance related criteria in their compensation and bonus systems and to report on the implementation of those measures to the DOJ. Under the Pilot Program, the DOJ will also reduce penalties for a company up to the amount of compensation it is able to claw back from employees during the resolution term, provided the company fully cooperates and timely and appropriately remediates.[35] Recent corporate resolutions highlight the DOJ's use of the new Pilot Program.[36]

— **Off-Channel Communications and Use of Personal Devices**: The DOJ announced its expectations for cooperation in investigations, including through updates to the Evaluation of Corporate Compliance

[29] Speech, "Acting Assistant Attorney General Nicole M. Argentieri Delivers Keynote Address at the 40th International Conference on the Foreign Corrupt Practices Act" (November 29, 2023), available here; Speech, "Assistant Attorney General Kenneth A. Polite, Jr. Delivers Remarks on Revisions to the Criminal Division's Corporate Enforcement Policy" (January 17, 2023), available here.

[30] DOJ, "The Criminal Division's Pilot Program Regarding Compensation Incentives and Clawbacks" (March 3, 2023) available here.

[31] Speech, "Deputy Attorney General Lisa Monaco Delivers Remarks at American Bar Association National Institute on White Collar Crime" (March 2, 2023), available here.

[32] *See also* our March 2023 alert memo on this topic, "Department of Justice Announces Revisions to Criminal Division Policies", available here

[33] DOJ, "Evaluation of Corporate Compliance Programs" (updated March 2023), at 12-14, available here; *see also* our March 2023 alert memo on this topic, "Department of Justice Announces Revisions to Criminal Division Policies", available here.

[34] *Id.*; *see also* DOJ, "The Criminal Division's Pilot Program Regarding Compensation Incentives and Clawbacks" (March 3, 2023) available here.

[35] *Id.*

[36] Press Release, "Corficolombiana to Pay $80M to Resolve Foreign Bribery Investigations" (August 10, 2023), available here; Press Release, "Albemarle To Pay Over $218M To Resolve Foreign Corrupt Practices Act Investigation" (September 29, 2023), available here; *see also* Speech, "Acting Assistant Attorney General Nicole M. Argentieri Delivers Remarks at the American Bar Association 10th Annual London White Collar Crime Institute" (October 10, 2023), available here.

Programs,[37] which now directs prosecutors to consider as part of their analysis the company's policies and procedures governing the use of personal and corporate devices (including messaging apps), the retention of electronic messages affecting its ability to conduct investigations, and notice that companies give employees about electronic data policies.[38] Consistent with the DOJ's Evaluation of Corporate Compliance Programs, prosecutors will take into consideration how companies deter risky behavior and foster a culture of compliance through their implementation of policies related to off-channel communications. Among other areas, the DOJ will review the types of electronic communication channels used by company employees to conduct business and the mechanisms the company has put in place to manage and preserve information contained with each communication channel.[39] In considering such policies, companies should work to ensure that they are consistent with the applicable labor and data privacy laws in jurisdictions in which they operate.

— **Mergers & Acquisitions Safe Harbor Policy:**[40] With the policy goals of encouraging greater investment in compliance and avoiding any deterrence of M&A activity more generally, the DOJ announced a new Department-wide safe harbor that may shield companies from criminal prosecution where misconduct is identified and the acquiring company timely discloses the misconduct to the DOJ.[41] Under the new policy, a company may qualify for a presumption of a declination, or a safe harbor, by (i) voluntarily disclosing criminal conduct within six months from the date of closing (regardless of whether the misconduct was discovered pre- or post-closing); (ii) cooperating with the DOJ's investigation; and (iii) fully remediating within one year from the date of closing.[42] In announcing the new policy, DAG Monaco made clear that the DOJ's "goal is simple: good companies – those that invest in strong compliance programs – will not be penalized for lawfully acquiring companies when they do their due diligence and discover and self-disclose misconduct."[43] The DOJ has highlighted two recent Corporate Enforcement Policy declinations in the context of M&A activity as examples of its approach in this area.[44]

DOJ leadership has consistently touted the value and importance of its international partnerships in investigating and prosecuting FCPA and other white collar cases and how it views foreign authorities as "force multipliers" in the fight against corruption.

FCPA

In 2023, the DOJ entered into six criminal corporate resolutions and issued two declinations under the Criminal Division's Corporate Enforcement and Voluntary Self-Disclosure Policy. One of those resolutions included a corporate guilty plea following the breach of a deferred prosecution agreement, as well as the

[37] DOJ, "Evaluation of Corporate Compliance Programs" (updated March 2023), available here.

[38] *See also* our March 2023 alert memo on this topic, "Department of Justice Announces Revisions to Criminal Division Policies", available here; *see also* Speech, "Assistant Attorney General Kenneth A. Polite, Jr. Delivers Remarks on Revisions to the Criminal Division's Corporate Enforcement Policy" (January 17, 2023), available here. In his speech, AAG Polite noted that the DOJ would not accept a refusal to produce communications from third-party messaging applications "at face value." He further cautioned that a company's answers to questions about accessibility of communications, or the lack of answers, may well affect the criminal resolution a company will have to enter into with the DOJ.

[39] DOJ, "Evaluation of Corporate Compliance Programs" (updated March 2023), at 17-18, available here.

[40] Speech, "Deputy Attorney General Lisa O. Monaco Announces New Safe Harbor Policy for Voluntary Self-Disclosures Made in Connection with Mergers and Acquisitions" (October 4, 2023), available here.

[41] *Id.*

[42] *See id.* The DOJ explained that these deadlines can be extended subject to a "reasonableness analysis," recognizing that the complexity of deals can differ and specific facts and circumstances may warrant extension; *See also* our October 2023 on this topic, "DOJ Announces Additional Guidance on Voluntary Self-Disclosure in M&A Context", available here.

[43] *Id.*

[44] *See, e.g.*, In re: Safran S.A. (CEP Declination Letter) (December 21, 2022), available here; In re: Lifecore Biomedical, Inc. (f/k/a Landec Corporation) (CEP Declination Letter) (November 16, 2023), available here.

extension of an ongoing monitorship.[45] This past year's FCPA resolutions also demonstrated the DOJ's efforts to put into practice the various policies released earlier in the year and previewed in past years.[46] One corporate resolution highlighted both the premium that the DOJ places on voluntary self-disclosure, as well as the requirement that self-reporting must be timely.[47] In that case, the company voluntarily self-disclosed the misconduct approximately 16 months after learning of the allegations, which the DOJ determined was not "reasonably prompt" under the Corporate Enforcement and Voluntary Self-Disclosure Policy.[48] Nevertheless, the DOJ highlighted the company's voluntary self-disclosure, substantial cooperation and significant remediation in resolving the matter through a non-prosecution agreement that awarded a 45% reduction from the low-end of the applicable penalty range, as well as the first ever penalty reduction based on the withholding of bonuses under the Pilot Program.[49] The DOJ also continues to expand its level of international cooperation and coordination with new foreign authorities, including coordinated resolutions with South Africa and, most recently, Colombia.[50] DOJ leadership has consistently touted the value and importance of its international partnerships in investigating and prosecuting FCPA and other white collar cases and how it views foreign authorities as "force multipliers" in the fight against corruption.[51] In November 2023, Acting Assistant Attorney General Nicole Argentieri announced the International Corporate Anti-Bribery (ICAB) initiative, which will build upon existing partnerships and develop new partnerships with foreign authorities, and will focus on particular regions that the DOJ views as having the greatest opportunity for coordination and case generation.[52]

The DOJ also continues to prioritize the prosecution of individuals in foreign bribery cases, as well as the use of multiple statutes to charge individuals, including the FCPA, money laundering, wire fraud and Travel Act.

The DOJ also continues to prioritize the prosecution of individuals in foreign bribery cases, as well as the use of multiple statutes to charge individuals, including the FCPA, money laundering, wire fraud and Travel Act. The last few years have shown an uptick in the number of foreign bribery-related trials,[53] with several additional foreign bribery trials scheduled for the coming year, including the January 2024 trial of Javier Aguilar, a former Houston-based manager and oil trader of a European energy trading company, in the Eastern District of New York.[54] Since 2018, the DOJ has announced charges against more than 150 individuals, and more than 100 individual convictions and guilty pleas, in foreign bribery-related cases.[55]

---

45 Press Release, "Ericsson to Plead Guilty and Pay Over $206M Following Breach of 2019 FCPA Deferred Prosecution Agreement" (March 2, 2023), available here.

46 *See* Speech, "Acting Assistant Attorney General Nicole M. Argentieri Delivers Remarks at the American Bar Association 10th Annual London White Collar Crime Institute" (October 10, 2023), available here.

47 DOJ Non-Prosecution Agreement, "Albemarle Corporation" (September 28, 2023), available here.

48 *Id.*; *see also* Speech, "Acting Assistant Attorney General Nicole M. Argentieri Delivers Remarks at the American Bar Association 10th Annual London White Collar Crime Institute" (October 10, 2023), available here.

49 *Id.*

50 Press Release, "Corficolombiana to Pay $80M to Resolve Foreign Bribery Investigations" (August 10, 2023), available here; Press Release, "ABB Agrees to Pay Over $315 Million to Resolve Coordinated Global Foreign Bribery Case" (December 2, 2022), available here.

51 Speech, "Acting Assistant Attorney General Nicole M. Argentieri Delivers Keynote Address at the 40th International Conference on the Foreign Corrupt Practices Act" (November 29, 2023), available here.

52 *Id.*

53 Press Release, "Former Goldman Sachs Investment Banker Convicted in Massive Bribery and Money Laundering Scheme" (April 8, 2022), available here; Press Release, "Former Venezuelan National Treasurer and Husband Convicted in International Bribery Scheme" (December 15, 2022), available here; Press Release, "Former Member of Barbados Parliament and Minister of Industry Found Guilty of Receiving and Laundering Bribes from Barbadian Insurance Company" (January 16, 2020), available here; Press Release, "Former President of Transportation Company Found Guilty of Violating the Foreign Corrupt Practices Act and Other Crimes" (November 22, 2019), available here; Press Release, "Former Senior Alstom Executive Convicted at Trial of Violating the Foreign Corrupt Practices Act, Money Laundering and Conspiracy" (November 8, 2019), available here.

54 Press Release, " Former Manager of Oil Trading Firm Charged in Money Laundering and Bribery Scheme" (September 22, 2020), available here.

55 DOJ FCPA Unit, "Enforcement Actions," available here; DOJ Fraud Section Year in Review 2018-2022, available here.

The new legislation is designed to prosecute foreign officials that solicit or receive bribes in exchange for being influenced or induced to perform or omit an official act or official duty, or conferring an improper advantage, in connection with obtaining or retaining business.

Finally at the end of 2023, Congress passed FEPA (the Foreign Extortion Prevention Act) as part of the 2024 National Defense Authorization Act. This legislation, signed into law by President Biden in late December 2023, will complement the FCPA by addressing the "demand side" of foreign bribery not covered by the FCPA.[56] Specifically, the new legislation is designed to prosecute foreign officials that solicit or receive bribes in exchange for being influenced or induced to perform or omit an official act or official duty, or conferring an improper advantage, in connection with obtaining or retaining business. How FEPA will be enforced will be a development that bears monitoring in the coming months.

Digital Assets

DOJ prosecutions of three of the biggest names in the digital asset space dominated the headlines in 2023. Following the collapse of the digital asset platform FTX in November 2022, FTX's founder Sam Bankman-Fried was brought to trial and found guilty in November 2023 of fraud and money laundering, among other charges, stemming from a wide-ranging scheme to misappropriate billions of dollars of customer funds.[57] In March 2023, Do Kwon, the founder of Terraform Labs, was charged with eight criminal counts of fraud related to, among other events, the collapse of the digital assets Terra and Luna in May 2022. Kwon spent most of 2023 in custody in Montenegro while pending extradition.[58] Most recently, Changpeng Zhao, the founder and CEO of Binance, the world's largest digital asset platform, pleaded guilty to failing to maintain an effective anti-money laundering program and resigned as the company's CEO, while the company agreed to pay over $4 billion to resolve the investigation into alleged violations.[59]

The DOJ's success in the digital asset space this year may serve as a model for its approach to other novel areas of technology in years to come.

The DOJ earned plaudits for its successful expedited prosecution of Bankman-Fried, and has established itself as a key government actor in the digital asset enforcement space, both through its National Cryptocurrency Enforcement Team, the Money Laundering and Asset Recovery Section and several U.S. Attorneys' Offices that now have experience with these cases. The DOJ's success in the digital asset space this year may serve as a model for its approach to other novel areas of technology in years to come.

Key Takeaways

Boards of directors should be prepared for investigations and enforcement actions designed to implement newly announced policy goals.

— Investigations and enforcement actions will continue at a sustained pace as both the SEC and DOJ bring new actions and resolve existing matters based on the

[56] *See also* our December 2023 alert memo on this topic, "Congress Passes Foreign Extortion Prevention Act to Prosecute Corrupt Foreign Officials", available here.

[57] Press Release, "Statement Of U.S. Attorney Damian Williams On The Conviction Of Samuel Bankman-Fried" (November 2, 2023), available here.

[58] Alexander Osipovich et al., "Do Kwon Arrested in Montenegro as U.S. Charges Crypto Fugitive With Fraud" The Wall Street Journal (March 23, 2023), available here; Ava Benny-Morrison et al, "Do Kwon Charged With Fraud by US Prosecutors in New York" Bloomberg, (March 23, 2023), available here; Alexander Osipovich and Marko Vešović, "Exclusive: Montenegro Plans to Extradite Fallen Crypto Tycoon Do Kwon to U.S." The Wall Street Journal, (December 7, 2023) available here.

[59] Press Release, "Binance and CEO Plead Guilty to Federal Charges in $4B Resolution" (November 21, 2023) available here.

various new rules and policies that they have issued during this past year.

— Expect continued and increased SEC litigation in the digital asset space against issuers, platforms and individuals. This trend is likely to continue until there is comprehensive legislation or legal clarity from the federal courts of appeals and Supreme Court, neither of which is likely to happen until 2025 at the earliest.

— The SEC will likely continue to focus on the investigation and litigation priorities it has laid out in recent years, including internal controls and disclosure violations—with a greater focus on AI, ESG and cybersecurity. Companies would be well-advised in the cybersecurity arena in particular to redouble efforts to make sure their cyber and disclosure controls are reasonably tailored to their businesses, and ensure that key actors are familiar with the SEC's new rules in the space.

— The DOJ will be focused on continued aggressive enforcement and resolution announcements that reflect the new policies announced this year. Companies should prepare by conducting ongoing reviews and monitoring of their compliance programs, as appropriate, including by considering the feasibility and practical implementation of clawback policies for executives, updating policies in connection with off-channel communications and the use of messaging applications or personal devices, and ensuring that their compliance programs appropriately prioritize the detection and reporting of potential wrongdoing to allow for timely escalation and remediation.

— Acquiring companies should continue to emphasize pre-close and post-close diligence focused on detecting and remediating misconduct of acquired companies to best position themselves to take advantage of new safe harbor provisions announced by the DOJ, as appropriate.

Delaware Courts Beef up *CareMark* Claims Involving Corporate Misconduct While Leaving Hot-Button Political and ESG Issues to the Boardroom

Roger A. Cooper
Partner
New York
racooper@cgsh.com

Mark E. McDonald
Partner
New York
memcdonald@cgsh.com

Andrew Khanarian
Associate
New York
akhanarian@cgsh.com

In 2023, Delaware courts continued to vigorously apply *Caremark*'s duty of oversight in cases involving corporate misconduct, expressly recognizing for the first time that such claims can be brought against officers in addition to directors. While a *Caremark* claim does not necessarily require illegal conduct, Delaware courts continue to make clear that knowing inaction when confronted with illegal conduct is often enough to satisfy its bad faith requirement. This emphasis on bad faith and misconduct may suggest a more functional approach to *Caremark* claims by Delaware courts, and a departure from the more formal categories of *Caremark* claims that Delaware courts relied on in the past. At the same time, we saw Delaware courts sidestep hot-button issues related to corporate political advocacy and defer to the business judgment of boards in order to navigate those sometimes controversial issues. Finally, we ended 2023 with an uncertain understanding of the scope of *MFW* review, which has expanded beyond the squeeze-out context in recent years. The Delaware Supreme Court is currently considering whether to cut back on such "*MFW* creep."

This emphasis on bad faith and misconduct may suggest a more functional approach to *Caremark* claims by Delaware courts, and a departure from the more formal categories of *Caremark* claims that Delaware courts relied on in the past.

Chancery Court Confirms *Caremark* Duties Extend To Officers, Leans Into More Functional Caremark Framework

In one of its most significant decisions of 2023, the Delaware Chancery Court in *In re McDonald's Corp. S'holder Derivative Litig.*[1] confirmed that officers owe a duty of oversight. Vice Chancellor Laster acknowledged that Delaware's courts had never expressly extended so-called *Caremark* duties to officers, as opposed to directors, but nonetheless held that *Caremark*'s reasoning for imposing a duty of oversight on directors applied equally to officers. Vice Chancellor Laster did, however, cabin the *Caremark* duty of officers to their area of authority and reiterated that such claims require a showing of bad faith, regardless of whether officers are subject to exculpation under Delaware General Corporation Law § 102(b)(7). Turning to the facts of the case, the Chancery Court found that plaintiffs adequately pleaded bad faith on the part of an officer based on his knowledge of red flags concerning pervasive sexual harassment at the company and his own engagement in sexual harassment. The Chancery Court further found that defendant's engaging in sexual harassment at the company was not just evidence of his knowledge, but also a breach of fiduciary duty in and of itself.

A few months later, the Chancery Court heard a *Caremark* claim against directors and officers of Walmart for their failure to oversee the distribution of prescription opioids at Walmart facilities in violation of prior settlements and federal law.[2] Because the defendants moved to dismiss the claims on demand futility grounds, a substantial likelihood of liability on the part of a majority of directors was sufficient to allow the claims to proceed. Vice Chancellor Laster found that the plaintiffs adequately pleaded that the majority of Walmart's directors faced potential *Caremark* liability with respect to a bulk of the claims because of their knowing disregard of serious compliance issues, and Vice Chancellor Laster therefore refused to dismiss those claims on demand futility grounds. Notably, Chancellor Laster discarded the three traditional categories of *Caremark* claims—so-called *Massey* claims, Red-Flag claims, and Information-Systems claims—in favor of a unified bad faith analysis. And while the Chancery Court stopped short of saying that a violation law was required for such a claim, it found sufficient allegations that Walmart's directors and officers consciously ignored the company's noncompliance with law.

Read together, *McDonalds*, *Walton* and *Segway* reflect both an expansion of *Caremark* claims to new actors as well as an renewed emphasis on their traditional principles and limits.

The Chancery Court's recognition that officers owe a duty of oversight, however, did not lower the standard for such claims. In *Segway*,[3] Vice Chancellor Will dismissed a *Caremark* claim against the president of a personal transportation device company for failing to recognize "financial struggles" at the company. Emphasizing the requirement that a *Caremark* claim plead a lack of good faith to detect "central compliance risks" within an officer's remit, Vice Chancellor Will stressed that "[t]he *Caremark* doctrine is not a tool to hold fiduciaries liable for everyday business problems." Vice Chancellor Will notably distinguished *McDonalds* by pointing out that plaintiffs here failed to plead knowledge of any violations of law.

Read together, *McDonalds*, *Walton* and *Segway* reflect both an expansion of *Caremark* claims to new actors as well as an renewed emphasis on their traditional principles and limits. Illegality and misconduct continue to feature prominently in a more functional analysis that

1 In re McDonald's Corp. S'holder Derivative Litig., 289 A.3d 343 (Del. Ch. 2023).

2 Ontario Provincial Council of Carpenters' Pension Tr. Fund v. Walton, No. 2021-0827-JTL, 2023 WL 3093500 (Del. Ch. Apr. 26, 2023).

3 Segway Inc. v. Cai, No. 2022-1110-LWW, 2023 WL 8643017 (Del. Ch. Dec. 14, 2023).

focuses on whether directors and officers participated in, knew of, or were willfully blind to such conduct.

Chancery Court Knocks Down Section 220 Claim Over Response To Controversial Florida Law

In *Simeone v. Walt Disney Company*,[4] the Delaware Chancery Court addressed a Section 220 request directed at records concerning Disney's opposition to a Florida law limiting instruction on sexual orientation and gender identity in Florida schools. Vice Chancellor Will held that the stockholder lacked a proper purpose for demanding the records, reasoning that the requests were actually driven by the stockholder's counsel. Vice Chancellor Will further held that the stated reason for the request, which was understanding Disney's response to the Florida law, lacked a credible basis of wrongdoing. To the contrary, the Vice Chancellor found the actions of the board to be precisely the type of decisions best entrusted to its business judgment.

Delaware courts appear hesitant to order the release of records that are loosely related to a company's business operations or financial performance, especially when those requests touch upon political or ESG issues.

Vice Chancellor Will reached a different result in *Greenlight Capital Offshore Partners, Ltd. v. Brighthouse Financial, Inc.*[5] and partially allowed the request. The plaintiff hedge fund in that case filed a books and records request for information it claimed that it needed to value its shares in the company. Even though the company insisted that the stockholder was motivated by activism, Vice Chancellor Will found any such ulterior motive to be irrelevant and ordered the partial release of records. Vice Chancellor Will was satisfied that there was at least one legitimate purpose for the request, in part because Delaware courts have recognized requests for share valuation purposes to be proper, in contrast to *Walt Disney* where she found the only stated stockholder purpose to be pretextual.

While Delaware courts continue to scrutinize a stockholder's stated purpose for a Section 220 request, the subject matter of the request appears to be an important factor in that analysis. Delaware courts appear hesitant to order the release of records that are loosely related to a company's business operations or financial performance, especially when those requests touch upon political or ESG issues. This approach to Section 220 requests is consistent with the Delaware courts' focus on providing robust remedies in instances of misconduct while deferring to boards on potentially controversial political or ESG issues.

Important *MFW* Questions Remain For Next Year

At the end of 2023, the Delaware Supreme Court heard arguments in *In re Match Grp., Inc. Derivative Litig.*,[6] a case set to decide whether conflicted transactions outside of the squeeze-out merger context must be approved by both an independent committee and a majority of minority shareholders in order to avoid entire fairness review, or whether it is enough for such transactions to use just one so-called "cleansing mechanism"—(1) approval by a majority of independent directors, (2) approval by a special committee of independent directors or (3) approval by a majority of disinterested shareholders—to get the benefit of business judgment review. Following the emergence of the *MFW* standard in 2014,[7] courts have steadily increased its application to a growing number of conflicted transactions beyond squeeze-out mergers (so-called "*MFW* creep"). The Delaware Supreme

[4] Simeone v. Walt Disney Co., 302 A.3d 956 (Del. Ch. 2023).

[5] Greenlight Cap. Offshore Partners, Ltd. v. Brighthouse Fin., Inc., No. 2022-1067-LWW, 2023 WL 8009057 (Del. Ch. Nov. 20, 2023).

[6] In re Match Grp., Inc. Derivative Litig., No. 2020-0505-MTZ, 2022 WL 3970159 (Del. Ch. Sept. 1, 2022).

[7] *See* Kahn v. M&F Worldwide Corp., 88 A.3d 635 (Del. 2014).

Court's decision to hear the case raises the possibility that boards may be able to avoid entire fairness review with fewer procedural hurdles than the *MFW* standard requires.

While this question will be answered in the coming year, 2023 already saw two decisions that arguably chip away at the centrality of the *MFW* process. In *In re Tesla Motors, Inc. S'holder Litig.*,[8] the Delaware Supreme Court held that Tesla satisfied the strenuous entire fairness standard with respect to its purchase of a solar company. Notably, the Delaware Supreme Court found that Tesla's failure to satisfy *MFW*'s procedural requirements did not imply lack of entire fairness. On the flipside of the same coin, in *HBK Master Fund v. Pivitol*,[9] the Chancery Court found the merger price resulting from a transaction that did comply with *MFW* nonetheless was not sufficiently reliable to determine fair value for purposes of a subsequent appraisal action.

Delaware courts remain willing to apply existing principles in new ways to hold directors and officers accountable.

Key Takeaways For Boards In 2023

— Delaware courts remain focused on providing robust remedies for corporate misconduct. Where misconduct occurs, Delaware courts remain willing to apply existing principles in new ways to hold directors and officers accountable. Boards should expect increased shareholder suits following the public reporting of misconduct, especially when directors and officers have themselves engaged in such misconduct.

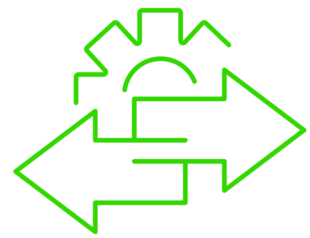
— Delaware courts remain hesitant to get involved in boardroom decision-making where there are no signs of misconduct, especially on hot-button political or ESG issues. But courts will not conduct a freewheeling inquiry into the motivation of Section 220 requests where stockholders present a legitimate purpose for the request.

— Companies with controlling stockholders should pay attention to whether the Delaware Supreme Court decides to cut back on the scope of *MFW* in 2024. That may impact the way such companies structure conflicted transactions outside of the squeeze-out context.

8 In re Tesla Motors, Inc. S'holder Litig., 298 A.3d 667 (Del. 2023).

9 HBK Master Fund L.P. v. Pivotal Software, Inc., No. 2020-0165-KSJM, 2023 WL 5199634 (Del. Ch. Aug. 14, 2023).

One Step Ahead: Restructuring Considerations in an Uncertain Economic Climate



Lisa M. Schweitzer
Partner
New York
lschweitzer@cgsh.com

Thomas Kessler
Partner
New York
tkessler@cgsh.com

As 2023 concludes, economic indicators remain mixed on whether there will be a recession or a soft landing over the next year. Either way, it is likely that a significant number of companies, across industries, will need to restructure their financial debt and operations. 2023 brought a significant increase in chapter 11 filings, with a 61% percent increase compared to the same period in 2022,[2] and filings across industries, including such notable companies as Bed Bath & Beyond, Envision Healthcare, Rite Aid and WeWork. Other companies have avoided formal bankruptcy filings by undertaking liability management transactions that increase near-term liquidity through additional borrowings. However, as several high profile filings this year have shown, it is likely that many of these transactions may simply delay, rather than prevent, bankruptcy filings in the future.

Companies can and should monitor for early signs of distress in order to develop a comprehensive strategy to minimize the impact of the financial distress of a key supplier, customer or other industry participant on its business and operations.

The current climate presents an ideal time for all companies to refresh their internal planning and to proactively consider the risks and opportunities that are presented when suppliers, customers and competitors encounter financial distress.

* The authors would like to thank Sabrina Bremmer for her contribution to this piece.

2 Epiq Global, "Year-to-Date Commercial Chapter 11 Filings Increased 61 Percent Compared To Same Period Last Year" (October 3, 2023), available here.

Early Planning for Potential Counterparty Distress

While free-fall bankruptcies make headline news, in most cases a company has experienced financial distress for a significant period of time before deciding to file for bankruptcy. Companies can and should monitor for early signs of distress in order to develop a comprehensive strategy to minimize the impact of the financial distress of a key supplier, customer or other industry participant on its business and operations.

In particular, management should be monitoring for early signs of potential distress and planning accordingly, and boards should oversee this process, including the following types of actions:

— **Stretching of trade terms** – Recent financial failures have been largely driven by near-term liquidity shortages. Companies should consider whether any request to renegotiate payment terms or noticeable changes in payment patterns could be signals of potential financial stress, and whether the larger commercial relationship could be at risk in the near or medium-term.

In negotiating the amendments of contract terms, companies should account for the potential impact of a subsequent bankruptcy filing on such amendments, and whether they may be forced to make further concessions later or whether any such amendments could be challenged in a bankruptcy proceeding.

— **Renegotiation of material commercial contracts** – For many companies, their long term supply and customer contracts do not match their current business models, including as a result of external factors, such as the rising costs of materials and labor, shifting customer demand for their goods and services, regulatory developments or other changes in their business operations (such as the increasing move to remote work). Companies may be approached to renegotiate these contracts either consensually or against a backdrop threat that contract amendments are necessary to ward off a larger failure. In negotiating the amendments of contract terms, companies should account for the potential impact of a subsequent bankruptcy filing on such amendments, and whether they may be forced to make further concessions later or whether any such amendments could be challenged in a bankruptcy proceeding.

- Companies also should review and consider the effectiveness of their own contractual default and termination rights under existing contracts with major counterparties that may be in distress. The right to enforce termination rights tied to bankruptcy filings and the financial condition of the counterparty, or that require notice and waiting periods, may not be fully enforceable in a bankruptcy scenario.

— **Readiness for an actual bankruptcy filing** – If a supplier or customer files for bankruptcy, it is important to be ready to react and mobilize from the start of the case in order to be best positioned throughout the process.

- **Initial bankruptcy relief** – Most debtors signal their restructuring strategy in their first day filings, including whether they intend to reorganize, pursue a sale or liquidate their business. They also may obtain court relief to pay select creditors that could affect other creditors. Companies should monitor the debtor's filings early on and engage of counsel to position themselves to mitigate the impact of a filing.

- **Planning for a sale** – Bidders have the right to cherry-pick assets and contracts in a bankruptcy sale process. Contracts that are taken by a buyer also have to be "cured" or be made current. It is important for companies to be proactive in best positioning their contracts to be assigned, or to be ready to oppose such an assignment if that is their preferred strategy.

Companies should not wait to consider the risk of the loss of their contracts in a bankruptcy and/or the concessions that may be requested, as well as the strategic leverage they may have in a case as a key supplier or customer whose contracts are essential for a successful reorganization.

- **Assumption and rejection of contracts** – A debtor in bankruptcy has the opportunity to reject its existing contracts and leases, which leaves the counterparty with unsecured claims for damages flowing from such rejection. This tool enables a debtor to both shed unfavorable contracts and attempt to extract consensual modifications of its agreements with others. Companies should not wait to consider the risk of the loss of their contracts in a bankruptcy and/or the concessions that may be requested, as well as the strategic leverage they may have in a case as a key supplier or customer whose contracts are essential for a successful reorganization.

- **The official creditors committee** – A committee is appointed at the start of each case to advocate for the interests of unsecured creditors, which is comprised of a mix of the largest unsecured creditors willing to serve and where the fees of the committee's professionals are funded by the debtor. Companies should consider serving on the committee as a way to further advance the interests of unsecured creditors in the case, including with respect to the direction of the reorganization and the treatment of unsecured claims.

— **Avoiding hindsight challenges** – In bankruptcy proceedings, a debtor may seek to claw back payments made to counterparties prior to filing or to extract further value through the pursuit of claims for preference (tied to counterparties having received payments or additional security outside of the ordinary course in the months prior to the bankruptcy) and fraudulent conveyance (for transactions in the years prior to the bankruptcy filing where fair value or reasonably equivalent value was not received by the debtor company at a time it was insolvent).

- Companies should take extra care when transacting with a party potentially in financial distress to ensure that transactions – particularly extraordinary transactions such as sales or acquisitions and the settlement of claims – are conducted in good-faith, at arms-length and for reasonably equivalent value.

Seize the Day: How a Counterparty's Financial Distress Could Create Opportunities

In many circumstances, a key supplier or customer's financial distress is a cause for concern and defensive planning. However, in times of economic turmoil, companies should also proactively consider opportunities that may be realized from other market participants' financial distress. In particular:

Companies should proactively consider whether there are opportunities for acquisitions of other market participants, and whether they can potentially initiate the process through an unsolicited offer where there may be significant first mover advantages in a fluid situation.

— **Acquisition opportunities** – While a company experiencing financial distress may pursue refinancings and operational restructurings as a first line strategy, to the extent such strategies do not prove successful the company may need to initiate a sale process to avoid having to turn itself over to its lenders. Other strategic players may be best positioned to act quickly in purchasing assets due to their ability to do discrete diligence and to close a transaction quickly. Companies should proactively consider whether there are opportunities for acquisitions of other market participants, and whether they can potentially initiate the process through an unsolicited offer where there may be significant first mover advantages in a fluid situation. There are significant considerations surrounding the decision whether to engage in acquisition transactions with a distressed counterparty outside of bankruptcy, as well as the strategy for pursuing acquisitions in bankruptcy auctions, where outside counsel can help companies best position themselves to succeed in their acquisition strategy.

— **Other opportunities** – To the extent companies are unable or uninterested in acquiring assets, other opportunities may exist including the chance to move customers from a competitor to their own business, to improve their position with common suppliers and to hire key employees who are laid off or otherwise looking to move away from a failing company. Given that these situations tend to unfold over time and are very fluid, a company may realize the most opportunities by developing a strategic plan early, monitoring the situation as it unfolds and remaining nimble and flexible in reshaping their acquisition strategy as the target's financial health may deteriorate and the situation may evolve either in or outside of a formal proceeding.

Self-Monitoring: Financially Healthy Companies Should Remain Alert as to Potential Risks to their Own Business

Even healthy companies should do their own periodic check-ups to identify potential financial and operational risks to their business and to ensure reporting and planning accounts for potential risks including market and industry changes.

It is prudent for management, with the oversight of the board, to regularly:

— Review the company's liquidity horizon and debt maturities, including to consider the expected strategy for addressing future capital needs, potential market alternatives that may provide additional liquidity or lower cost capital (such as liability management transactions) and the potential market and corporate risks that could affect the availability or cost of future capital.

— Monitor any contingent liabilities, including unasserted claims and legacy liabilities, that may affect the company's performance or result in significant financial liabilities, and consider the availability of structuring transactions that could be implemented to manage and isolate such liabilities over time.

— Refresh disclosed risk factors to include potential risks associated with industry changes, material supplier and customer risks, the existence of legacy and contingent liabilities and potential changes in the availability and cost of capital and consumer demand, among other things, as part of the preparation of public reporting.

As companies wait to see how the financial markets and industry outlook will unfold in 2024, they can take the above proactive and defensive planning steps to best position themselves to address industry distress, both to minimize its impact on their own financial health and to realize strategic opportunities as they may arise.

Regulatory Developments to Watch: Non Competes and ERISA

Elizabeth Dyer
Partner
New York
edyer@cgsh.com

Michael J. Albano
Partner
New York
malbano@cgsh.com

Alan M. Levine
Partner
New York
alevine@cgsh.com

Irene Kwon
Law Clerk
New York
ikwon@cgsh.com

Erin McKissick
Law Clerk
New York
emckissick@cgsh.com

Though perhaps not top of the agenda for boards of directors in 2023, there have been significant developments in two unrelated but important areas that boards should be mindful of heading into 2024—the increasing efforts to eliminate (or at least weaken) employee non-competition restrictions and regulatory developments in the ERISA pension plan fiduciary space.

Non-Competes

2023 saw a surge in significant developments restricting non-compete agreements and other restrictive covenants, both from federal agencies and state legislatures. Many of these developments are still unfolding and the trend toward restriction is likely to continue throughout 2024.

FTC Rule Proposal

In early 2023, the Federal Trade Commission (FTC) proposed a rule that would ban employers from entering into any non-competes with workers, as well as agreements that "have the effect of prohibiting the worker from seeking or accepting employment."[1] The rule would also require employers to rescind all existing non-competes by written notice. The sole exception

[1] § 910.1(b)(2). For a summary of the FTC's proposed rule, *see* our January 2023 alert memo available here.

would be for sale of business agreements, where the employee restricted by the non-compete owned at least 25% of the business sold.[2] The vote on this rule has been postponed until April 2024 at the earliest, and it is expected that there will be several legal challenges to the rule if it is adopted.

Since the issuance of the memo, we have seen only one reported complaint filed, by the NLRB's Cincinnati Regional Office, charging that an employer's use of restrictive covenants which applied to employees constituted unfair labor practices.

NLRB Enforcement

In May 2023, the General Counsel to the National Labor Relations Board (the NLRB), Jennifer A. Abruzzo, issued a memorandum stating that most non-compete agreements violate the National Labor Relations Act (the Act).[3] Although the memo is not binding on the NLRB, General Counsel Abruzzo directed the NLRB's regional offices to investigate employers using non-competes to determine whether their usage is "overbroad". While it was a striking action by the General Counsel, since the issuance of the memo, we have seen only one reported complaint filed, by the NLRB's Cincinnati Regional Office, charging that an employer's use of restrictive covenants which applied to employees constituted unfair labor practices.[4]

State Developments

Also in May, 2023, Minnesota became the 4th U.S. state to ban all employee non-competes (joining California, North Dakota and Oklahoma), with a new law that went into effect on July 1, 2023.[5] The law bans all agreements that impose post-termination restrictions on employees from performing work (i) for another employer for a specified period; (ii) in a specified geographical area; or (iii) for another employer in a capacity that is similar to the employee's work for the employer that is a party to the agreement.[6] While the law is not retroactive and does not affect other employee restrictions, such as confidentiality and non-solicitation covenants, it does bar employers from utilizing choice-of-law or choice-of-venue clauses in agreements with Minnesota employees and independent contractors in an attempt to use a more favorable state's law as a workaround.

New York threatened to follow suit when, in June 2023, its State legislature passed a bill banning all non-competes entered into on or after 30 days following the bill's enactment, including those entered into by employees or in connection with the sale of a business.[7] The bill would have covered any person who performs work or services for another person where the individual is in a position of economic dependence on that other person.[8] Governor Kathy Hochul has since vetoed the bill, but has made statements to reporters indicating her preference for finding a compromise that would ban non-competes for those earning less than $250,000 per year.[9]

Finally, notwithstanding the fact that California was one of the early adopters of a total ban on non-competes,[10] Governor Gavin Newsom signed into law two new bills, Senate Bill 699 (SB 699) and Assembly Bill 1076 (AB 1076), in September and October of 2023 respectively, strengthening the protections of California's existing statutory prohibitions. Both went into effect on January 1, 2024. Under SB 699, prohibited non-competes are void "regardless of where and when the contract was signed," and employees (current, former, and potential)

2 § 910.3.

3 *Non-Compete Agreements that Violate the National Labor Relations Act*, Memorandum GC 23-08 (May 30, 2023).

4 NLRB Office of Public Affairs, "Region 9-Cincinnati Issues Complaint Alleging Unlawful Non-Compete and Training Repayment Agreement Provisions (TRAPs)" (September 7, 2023), available here.

5 *See* our June blog post for our summary of the Minnesota law, available here.

6 Minn. Stat. § 181.988.

7 *See* our June alert memo for our summary of the New York bill, available here.

8 New York State Senate Bill S3100A.

9 *See* our December alert memo for our summary of the Governor's statements, available here.

10 California Business and Professions Code § 16600.

can bring private actions for injunctive relief, actual damages and reasonable attorney's fees and costs. AB 1076 requires employers to issue notice to all current and former employees employed after January 1, 2022 and subject to a non-compete in violation of California's prohibition that their restrictions are void, by February 14, 2024.

Next Steps

Employers should catalog where employees are located and be prepared to track both current and former employee mobility to ensure they remain in compliance, determine whether any employees in California should receive the required notice by February, review and revise form agreements for any potentially void non-compete clauses, and continue to monitor these and other developments over the coming year.

The DOL's Continued Regulatory Initiatives: A New Fiduciary Rule, Proposed QPAM Amendments and ESG-Related Guidance

The Department of Labor (the DOL) has had another active year – a trend we predict will continue into 2024. This high-level overview of a few notable DOL regulatory initiatives from 2023 should be useful for board and management teams alike.

The DOL's Proposed Amendment to the Definition of an Investment Advice Fiduciary

In October of 2023, the DOL proposed a new rule (the Proposed Rule) that would redefine who constitutes an "investment advice" fiduciary under the Employee Retirement Income Security Act of 1974, as amended (ERISA).[11] The DOL intends many of the proposed changes to ensure that rollover recommendations provided to participants and beneficiaries of 401(k) plans and individual retirement accounts fall under the umbrella of fiduciary "investment advice." However, the changes ushered in by the Proposed Rule are much broader in scope and do not include any exclusions or safe harbors. If the Proposed Rule is finalized as currently formulated, companies sponsoring ERISA plans and a wide variety of service providers and financial institutions will need to determine which actions (including regular marketing and sales activities) could be deemed to be fiduciary "investment advice" going forward.

The Proposed Rule is subject to a 60-day notice and comment period. Public hearings took place in early December and written comments were due to the DOL on January 2, 2024. Many industry groups, financial institutions, investment advisers and organizations representing ERISA plans and plan sponsors have submitted comment letters to the DOL. Given that no final rule has yet been adopted, no immediate action is required at this time. However, if the Proposed Rule is finalized, companies sponsoring ERISA plans and financial institutions providing services to ERISA plans should consider surveying the impact on existing arrangements and whether changes will be needed to manage the risks associated with fiduciary status under the more expansive rule.

Depending on the substance of the final amendments, we may see less reliance on the QPAM Exemption across a broad range of transactions, which could have a chilling effect on the willingness of service providers to enter into contracts with ERISA plans.

The DOL's Proposed Amendment to the QPAM Exemption

Companies sponsoring ERISA plans and service providers to such plans frequently rely on Prohibited Transaction Exemption 84-14, as amended (the QPAM Exemption). As summarized in our Selected Issues for Boards of Directors for 2023, the DOL proposed material changes to the QPAM Exemption in July of 2022 that would

[11] *See* our November alert memo for a summary of the Proposed Rule, available here.

impact the ability of plan sponsor and service providers alike to rely on the QPAM Exemption.[12] The DOL received hundreds of comments and held several days of public hearings on the proposed amendments. Despite vocal criticism regarding the proposed amendments, it is widely anticipated that the DOL will seek to finalize the amendments to the QPAM Exemption.

Depending on the substance of the final amendments, we may see less reliance on the QPAM Exemption across a broad range of transactions, which could have a chilling effect on the willingness of service providers to enter into contracts with ERISA plans. Compliance with the amended QPAM Exemption is likely to be costly to plan sponsors and service providers alike, and the increased risk and cost of relying on the QPAM Exemption could result in financial institutions and asset managers charging ERISA plans higher fees for investment management services and financial transactions.

The DOL's ESG Guidance

In November of 2022, the DOL released its final rule (the Final Rule) clarifying the application of ERISA's fiduciary duties to the selection of investments and investment courses of action.[13] The Final Rule reaffirms a bedrock principle under ERISA's duties of prudence and loyalty – when selecting investments and/or investment courses of action, plan fiduciaries must focus on the relevant risk-return factors and may not subordinate the interests of participants and beneficiaries to objectives unrelated to the provision of benefits under the plan (*e.g.*, by reducing investment returns and/or increasing investment risks).

In September 2023, the DOL released a new Advisory Opinion addressing the retention of diverse managers by ERISA plans sponsored by a financial institution; in connection with the retention of these managers, the financial institution is expected to pay all or part of the investment management fees otherwise payable by the ERISA plans.[14] The retention of diverse managers by the ERISA plans is part of the financial institution's broader strategic initiative to address social issues, including the underrepresentation of diverse managers in the asset management space.[15] The DOL addressed the question of whether the investment committees for the ERISA plans could consider the reduced management fees associated with the diverse managers in connection with its selection process. The DOL concluded that, while it would be inconsistent with ERISA for the investment committees to exercise their fiduciary duties to select investment managers that further the financial institution's public policy goals, an analysis of the fees payable by the ERISA plans for investment management services would be a relevant factor to consider in connection with a prudent selection process.

ERISA plan fiduciaries continue to be bound by ERISA's duties of prudence and loyalty and this Advisory Opinion does not materially change the legal landscape regarding when and how ESG-related factors can be incorporated into a prudent selection process.

This Advisory Opinion, which garnered headlines, may result in increased questions around ESG-focused investments or, in the case of 401(k) plans, pressure to make ESG-focused investment options available to plan participants. ERISA plan fiduciaries continue to be bound by ERISA's duties of prudence and loyalty and this Advisory Opinion does not materially change the legal landscape regarding when and how ESG-related factors can be incorporated into a prudent selection process.

12 *See* 87 Fed. Reg. 73866 (December 1, 2022); *see also* our January 2023 publication, Selected Issues for Boards of Directors 2023 for a summary of the proposed amendments to the QPAM Exemption, available here.

13 *See* our December 2022 alert memo for a summary of the final rule, available here.

14 *See* DOL Advisory Opinion 2023-01A (AO 2023-01A), available here.

15 *See* AO 2023-01A, which describes the program as "a comprehensive approach to increasing investment in Black-owned business, advancing racial equity practices in the financial services industry, providing greater access to banking and credit in communities of color, and expanding home ownership among Black Americans." AO 2023-01A states that "diverse managers" are those with minority/female ownership of a specified percentage as measured by a third party database.

Next Steps

ERISA plan sponsors, fiduciaries, and service providers should continue to monitor these and other DOL initiatives over the coming year.

2024 Antitrust Update: Agencies Sharpen Their Teeth, But Is It All Bark and No Bite?

Antitrust in 2023 was marked by a series of policy developments—some still nascent, some ripe for enforcement for the first time. In the U.S., the FTC and DOJ finalized their drastically transformed merger guidelines. In the EU, landmark new digital regulations became applicable for the first time. And the UK government introduced a bill promising major new digital and consumer protection rules.

Regulators may be getting new tools, but the question for 2024 will be how they use them. Enforcement remained healthy on both sides of the Atlantic last year and we can expect that to continue. U.S. agencies continued their focus on allegedly anticompetitive labor and employment agreements, while seeing mixed results in their enforcement litigations. While the UK's Competition and Markets Authority (CMA) showed signs of relaxing its interventionist stance, it remained unafraid to pursue novel theories of harm.

Other topics to watch this year include the antitrust response to the rise of artificial intelligence, the EU's new foreign subsidies regime and the continued complexity of cross-border merger control with its often-divergent outcomes.

U.S. Antitrust Developments

D. Bruce Hoffman
Partner
Washington, D.C.
bhoffman@cgsh.com

Kenneth Reinker
Partner
Washington, D.C.
kreinker@cgsh.com

Daniel P. Culley
Partner
Washington, D.C.
dculley@cgsh.com

Magd Lhroob
Associate
Washington, D.C
mlhroob@cgsh.com

FTC/Litigation Updates: Intensified Rhetoric, Few Legal Victories

Aggressive posturing by US enforcers isn't leading overwhelmingly to court wins, though the US agencies obtained better litigation results than they did in 2022. 2023 also brought the same rhetoric and intense scrutiny of transactions as we saw in 2022. And yet, current enforcement numbers remain far below those of past administrations. In previous years, antitrust agencies have challenged the legality of 3 to 4 percent of reviewed transactions; while the current administration has challenged under 2 percent. We expect merging parties will still face aggressive regulators in 2024. The FTC and DOJ are willing to challenge and litigate hard cases under novel theories of antitrust harm, and use the second request process to find and enforce other violations. Meanwhile, dealmakers are responding with higher break fees and longer termination dates, with 18 to 24 months becoming more common in large, complex deals.

The new guidelines specifically call for evaluations of any prior enforcement, restrictive agreements, worker switching costs and a loss of compensation potential. However, the guidelines themselves have no legal effect—they are simply statements of internal agency policy.

In an interview with The Wall Street Journal, Assistant Attorney General with the U.S. Justice Department's Antitrust Division Jonathan Kanter suggested the agency is digging more deeply into minority acquisitions and board seat appointments. He says, "If companies are making minority investments and obtaining board seats, and those investments and those board seats lead to the kind of control that would be troubling in the context of a merger or an agreement—absolutely we should take a look. If that is becoming a more common playbook, then it is incumbent on us as enforcers to adapt."[1]

Merger Guidelines

The finalized merger guidelines represent a drastic shift in the merger investigations process. The guidelines depart from decades of practice by introducing novel presumptions that could make it harder for mergers to obtain regulatory clearance from the agencies. The agency standard concentrations are significantly lower, there are now new provisions addressing vertical deals and an expansion of the evaluation of transactions' impact on labor and employment issues. The new guidelines specifically call for evaluations of any prior enforcement, restrictive agreements, worker switching costs and a loss of compensation potential. However, the guidelines themselves have no legal effect—they are simply statements of internal agency policy. So, while they provide more insight into the thinking of the current leadership, whether they have any impact on courts remains to be seen.

If adopted, the proposals could create a dynamic where the agencies may reject filings for purported technical non-compliance or encourage parties to extensively consult with staff prior to submitting filings or even to submit draft filings for "pre-filing review."

HSR Form Changes

The US agencies also proposed massive changes to HSR filing requirements. If adopted—and significant pushback is expected—the proposals would increase the burden in each area where information is currently required and would add numerous additional requirements. In addition, given the vagueness of the

[1] Wall Street Journal, "What's Behind the U.S. Government's New Antitrust Focus" (December 13, 2023), available here.

new requirements, if adopted, the proposals could create a dynamic where the agencies may reject filings for purported technical non-compliance or encourage parties to extensively consult with staff prior to submitting filings or even to submit draft filings for "pre-filing review." This system may be somewhat similar to the filing system in Europe, but the US filing requirements apply to a vastly larger array of transactions, the overwhelming majority of which present no antitrust issues. Thus, for decades the US system has focused on light up-front filing requirements, with in-depth review reserved for the tiny fraction (typically less than 3%) of filings that actually raise antitrust concerns. The current proposals would flip that on its head, imposing extensive burdens on all transactions—including the 97% or so of filings that raise no antitrust concerns.

Continued Focus on Labor and Employment Issues

In January 2023 the FTC proposed a near-total ban on noncompete agreements. This latest update in the FTC and DOJ's focus on labor and employment issues was announced simultaneously with enforcement actions accusing companies of abusing employment agreements to depress wages and limit competition. Industry officials and trade organizations were highly critical of the rule proposal and some doubt the FTC has legal authority to make the change.

After multiple court losses and market wide investigations trying to prosecute "no poach" violations, the agency recently moved to dismiss a matter involving healthcare workers in the Surgical Care Affiliates case, perhaps signalling a change in strategy by DOJ.

Section 8 Investigations

2023 has seen dozens of active investigations leading to more than fifteen director resignations. The FTC also had its first Section 8 enforcement action is more than 40 years. During an HSR investigation of the deal between Quantum Energy Partners and EQT, the agency identified a problematic board overlap and the potential for an exchange of confidential information. The FTC required the director to resign and the company to divest shares eliminating the risk of an illegal exchange of competitive information.

Safe Harbor Information Sharing

In 2023 both DOJ and FTC withdrew healthcare enforcement policy statements enforcement guidance that had been applied to information sharing for businesses generally. In announcing the withdrawal, Deputy Assistant Attorney General Doha Mekki asserted that the policy statements did not reflect the current modern business place and that the "safety zones" outlined in the guidelines have been misapplied in contexts and industries that were never contemplated by the guidance: "*…the Division is concerned that the factors do not consider the realities of a transformed industry and, therefore, understate the antitrust risks of competitors sharing competitively-sensitive information*."[2] She went on to explain the DOJ will now take a "case by case enforcement approach to better evaluate" whether information sharing may harm competition.

In September, the DOJ filed a lawsuit accusing Agri Stat of engaging in an illegal information exchange related to turkey, chicken and pork. This case follows a number of other antitrust cases brought by both the DOJ and by private plaintiffs relating to issues in these industries.

Constitutional Legal Challenges

The Supreme Court heard two cases impacting administrative proceedings at federal administrative agencies: (1) Axon v. FTC and SEC v. Cochran in a consolidated case; and (2) SEC v. Jarkesy.

On April 14, 2023, the Supreme Court unanimously held, in Axon and Cochran, that parties may raises challenges to the constitutionality of the structure of administrative agencies in federal court prior to the conclusion of administrative proceedings. The Supreme Court held that the "*review schemes set out in the Securities*

[2] *See* DOJ, "Principal Deputy Assistant Attorney General Doha Mekki of the Antitrust Division Delivers Remarks at GCR Live: Law Leaders Global 2023" (February 2, 2023), available here.

Exchange Act and Federal Trade Commission Act do not displace district court jurisdiction."[3]

The Supreme Court heard argument in the Jarkesky case on November 29th. The Jarkesy case claims that the SEC's use of ALJs violates the Constitution and denies the company the right to a jury trial despite being faced with civil penalties. While the Axon case primarily impacted how a challenge can be heard, the Jarkesy case may pose a greater threat to administrative litigation, at least where penalties are at issue.

In December 2023, the 5th U.S. Circuit Court of Appeals rejected, based on existing Supreme Court precedent, constitutional challenges to the FTC in the Illumina/Grail merger case.

Legislation

U.S. Congress has lost much of its momentum for addressing Big Tech and general antitrust reform, but there is a renewed push to regulate AI. The Senate Judiciary Committee held a hearing on AI and competition focusing mainly on pricing algorithms. AI applications like ChatGPT and other large language models are displaying new capabilities leaving legislators and regulators wondering if enforcement tools are keeping up with the technology. Some industry experts believe new laws and tools are needed, but with political gridlock in Washington we are unlikely to see major changes in the law any time soon.

Europe and ROW Antitrust Developments

Henry Mostyn
Partner
London
hmostyn@cgsh.com

Fay Davies
Associate
London
fdavies@cgsh.com

In Europe, digital regulation led the agenda for 2023 and the coming year looks to be no different. Other topics to watch are a new foreign subsidies regime, continued cross-border merger review complexity, and major new powers for digital regulation and consumer protection in the UK.

Digital Regulation Will Stay in the Headlines…

This year, the European Commission (EC) will start to enforce its landmark digital regulations for the first time.

The Digital Markets Act (DMA) and Digital Services Act (DSA) came into force in 2022. While the DMA introduces a set of "dos and don'ts" governing the behavior of "gatekeeper" digital platforms, the DSA focuses on the distribution of user-generated content online. Both regulations are designed to "create a safer digital space where the fundamental rights of users are protected and to establish a level playing field for businesses."[4]

In late 2023, the European Commission (EC) designated its first round of DMA "gatekeepers": Amazon, Apple, ByteDance, Google, Microsoft and Meta. These gatekeepers will have to follow the DMA's behavioral rules in respect of their designated services as of March 2024. We will likely see further gatekeeper designations this year as platforms continue to emerge and grow, and

[3] *See* Axon Enterprise, Inc v. Federal Trade Commission et al. (decided April 14, 2023), available here.

[4] *See* European Commission, "The Digital Services Act Package" (last updated December 7, 2023), available here.

we may even see the EC's first infringement decisions if it deems that gatekeepers are not compliant.

We will likely see further gatekeeper designations this year as platforms continue to emerge and grow, and we may even see the EC's first infringement decisions if it deems that gatekeepers are not compliant.

The world will be watching with interest as these far-reaching and unprecedented regulations play out for the first time. Jurisdictions like Japan, Australia and Turkey – in the midst of exploring their own digital regimes – will be paying particularly close attention.

…While Antitrust Regulators Will Keep a Close Eye on Artificial Intelligence

Artificial intelligence has been on the antitrust radar for a few years, but the "chatbot" explosion of 2023 caught the world by surprise. Regulators were nevertheless quick to react, and 2024 will likely witness the first attempts to regulate AI across competition, IP and other fields.

In the UK, the Competition and Markets Authority (CMA) launched a review into AI foundation models in May 2023. Its initial report focused on guiding principles rather than concrete regulatory proposals, but announced the beginning of "a significant programme of engagement" in the "UK, US and elsewhere."[5] CEO Sarah Cardell emphasised at the time that the CMA is "ready to intervene where necessary."[6] Her remarks were prescient: two months later the CMA published an invitation for comments on whether it should review the Microsoft/OpenAI partnership under UK merger laws.

EU legislators agreed the final text of the AI Act in late 2023 after last-minute changes to reflect the development of chatbots and the LLM-race. The Act will regulate both those that provide and those that deploy AI systems with an effect in the EU. And, doubtless keen to ensure that its new digital regulations do not become obsolete as soon as they launch, the EC has made clear that the DMA has "all the tools" it needs to "understand and regulate" AI.[7]

The CMA Sharpens Teeth in Digital Regulation and Consumer Law, but the Fate of Merger Control is Uncertain

In the UK, 2023 was marked by two themes pulling in opposite directions.

The first was the arrival of the Digital Markets, Competition, and Consumers Bill, and its promise of wide-ranging new powers for the CMA in digital regulation and consumer protection. If the Bill comes into force, as is expected later this year:

— The CMA (via a new Digital Markets Unit) will be able to impose bespoke conduct requirements on digital firms with "strategic market status" and make "pro-competitive interventions" to address these firms' market power. Financial penalties under the regime will be severe and the Digital Markets Unit will be able to apply to the court to disqualify individuals from holding company directorships in the UK.

According to CMA CEO Sarah Cardell, we will see a "watershed moment" in the UK's consumer protection regime. If the Bill becomes law, the CMA will for the first time be able to directly impose orders and fines for consumer law infringements (up to 10% of global annual turnover). If the Bill passes, the new regime will come into effect in late 2024 or 2025.

The second theme was the signs of a possible turning point in the CMA's merger enforcement. In the seven

5 CMA, "AI Foundation Models Review: Short Version" (September 18, 2023), available here.

6 CMA Press Release, "Proposed principles to guide competitive AI markets and protect consumers" (September 18, 2023), available here.

7 *See* Global Competition Review, "DMA can tackle AI concerns, Bacchiega says" (September 28, 2023), available here.

years since the Brexit vote, the CMA has established a reputation for being the most interventionist antitrust agency in the world, blocking or causing the abandonment of eight transactions since January 2019, including those with little UK nexus.

While we would expect the CMA to remain among the more interventionist agencies in the world, the Activision experience suggests that going forward it may become easier to find remedies to resolve the CMA's concerns, in particular if the CMA moderates its aversion to accepting behavioral remedies.

The events of 2023 suggested that this stance may be relaxing. Having blocked the Microsoft/Activision deal in April, the CMA took the highly unusual step of opening a new investigation into a "restructured" version of the transaction in August, eventually approving the deal in September based on behavioral remedies. While we would expect the CMA to remain among the more interventionist agencies in the world, the Activision experience suggests that going forward it may become easier to find remedies to resolve the CMA's concerns, in particular if the CMA moderates its aversion to accepting behavioral remedies.

The New Normal for Cross-Border Merger Review

2023 saw examples of significant divergence between EU and UK merger investigations. This has been a common thread since Brexit and it warrants the attention of companies involved in cross-border deals in Europe.

The CMA and EC reached contrasting conclusions on three high-profile transactions.

- The EC approved Microsoft's acquisition of Activision conditional on a behavioral commitment, but the CMA blocked the deal outright, arguing that the proposed behavioural remedies would be insufficient (before ultimately approving a restructured deal).
- The CMA approved the merger between Booking.com and Etraveli, while the EU rejected the parties' proposed remedies and blocked the deal.
- The CMA approved Broadcom's acquisition of VMware unconditionally at Phase 2, while the EC required behavioural commitments from Broadcom before allowing the deal.

Merging parties in cross-border deals will need to consider distinct strategies for each regulatory body, possibly including different proposals for remedies.

Competition Enforcement in Labor Markets: Talk Turns to Action?

Back in 2021, the EC announced plans to pay more attention to agreements restricting competition on the labor market.[8]

So far, enforcement action has been confined within Member State borders, including in relation to no-poaching agreements in Portugal and Lithuania.

In 2023, however, the EC updated its guidelines on horizontal cooperation agreements to consider wage-fixing as a by-object infringement, giving it the power to take a harder line on these agreements without needing to show an effect on competition. This suggests that EU-level enforcement may be on the agenda for 2024, bringing the EU in line with the US, where no-poach and similar agreements have long been a focus.

[8] EU Commission "A New Era of Cartel Enforcement, Margrethe Vestager," Speech, (October 22, 2021).

The EU Now Reviews Deals for Distortive Subsidies

The Foreign Subsidies Regulation (FSR) is now in effect, adding a further layer of regulatory review for M&A and public tenders in the EU. Companies that have material financial interactions with non-EU state entities – including arms-length commercial dealings – are obliged to notify large acquisitions and public procurement bids to the EC. Under the FSR, the EC will assess if businesses have received subsidies that distort competition in the internal market, and if so, whether redressive measures should be imposed.

The FSR is the first of its kind globally – no other jurisdiction regulates "foreign subsidies" on competition grounds. Due to the FSR's broad scope, over 30 transactions have been notified since the regime became fully operative in October 2023. Amid calls for better clarity, the EC has promised early guidance on how it will assess the distortive and positive effects of foreign subsidies in the first half of 2024, ahead of formal guidelines in 2026.[9]

[9] For more information on the FSR, see our Foreign Subsidies webpage available here.

Economic Sanctions: Developments and Lessons for Boards in 2024

Chase D. Kaniecki
Partner
Washington, D.C.
ckaniecki@cgsh.com

Samuel H. Chang
Associate
Washington, D.C.
sachang@cgsh.com

William S. Dawley
Associate
Washington, D.C.
wdawley@cgsh.com

Continued volatility in geopolitical events this past year and corresponding responses in sanctions policies highlight the importance of integrating economic sanctions considerations in board agendas for 2024. In particular, boards of directors should be aware of the increasing global collaboration among sanctions authorities as well as the continuing expansion and application of sanctions in new domains such as digital assets. Sanctions developments can be expected to be particularly fluid in 2024 with respect to China, Russia and Venezuela.

Responses to Global Conflict and Crises

In 2023, economic sanctions by the United States and its partners and allies continued to be a key component of conflict and crisis response.

For example, as the Russian offensive in Ukraine entered its second year, the United States, United Kingdom and European Union have maintained close coordination in the further imposition and enforcement of sanctions, in particular with respect to the enforcement of the price cap against Russian-origin crude oil and petroleum products.[1]

Also, in response to commitments made by representatives of Venezuelan President Maduro and the Unitary Platform relating to democratic elections and the release of prisoners, the U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC) suspended sanctions relating to oil and gas sector operations in Venezuela through April 18, 2024, authorized certain transactions involving the Venezuelan state-owned mining company and–consistent with private-sector sentiment and

---

[1] *See e.g.*, U.S. Department of the Treasury, "Price Cap Coalition Advisory for the Maritime Oil Industry and Related Sectors" (October 12, 2023), available here; U.S. Department of State, "United States Imposes Additional Sanctions and Export Controls on Russia in Coordination with International Partners" (May 19, 2023), available here. For additional information see our blog posts on Russia-Ukraine sanctions updates here, and here.

pressure–revoked a Trump-era ban on the ability of U.S. persons to purchase Petróleos de Venezuela, S.A. and Venezuelan sovereign bonds on the secondary market.[2] The U.S. government has threatened the reimposition of certain sanctions—most prominently the general license authorizing oil and gas transactions—if the Maduro regime fails to follow through with its commitments to take concrete steps toward a democratic election in 2024.

In addition, following the October 7, 2023 attack by Hamas against Israel, the United States imposed several rounds of sanctions, primarily targeting Hamas operatives and financial facilitators, including conduits for illicit funds. The United States stated its intention to continue imposing such sanctions in 2024 to disrupt Hamas's financial network, including through new sanctions authorities, as discussed below.[3]

Throughout 2023, the United States updated its sanctions guidance and enforcement posture relating to the joint price-cap on Russian crude oil and petroleum products in coordination with the price cap coalition countries.

Sanctions Coordination

The war in Ukraine has served as a catalyst for the Biden Administration's emphasis on incorporating multilateral coordination into its sanctions policy. For example, in May 2023, members of the G7 and other partners imposed additional sanctions on Russia in response to commitments made at the G7 Leader's Summit. Also, throughout 2023, the United States updated its sanctions guidance and enforcement posture relating to the joint price-cap on Russian crude oil and petroleum products in coordination with the price cap coalition countries.[4]

October 2023 marked the first year of the OFAC-UK Office of Financial Sanctions Implementation (OFSI) Enhanced Partnership between U.S. and UK sanctions authorities,[5] through which OFAC and OFSI coordinated at multiple levels of seniority to exchange best practices, align on sanctions implementation and shared objectives, and hold joint private-sector engagements (including the first round table with fintech and digital assets stakeholders). This partnership has manifested in concrete actions, including coordinated sanctions in response to the Israel-Hamas conflict,[6] as well as joint coordination with Canada in imposing new actions against several individuals and entities for supporting Myanmar's military regime.[7]

OFAC has similarly continued its bilateral EU partnership with the European External Action Service and the Directorate-General for Financial Stability, Financial Services and Capital Markets union. This coordination includes participation in the U.S.-EU Trade and Technology council, which continues to play a key role in coordinating action between the partners, particularly in the context of the war in Ukraine.

We expect that these communication channels, institutional structures and precedent established over the past two years will continue to facilitate and shape multilateral coordination on other issues.

---

2 U.S. Department of the Treasury, "Frequently Asked Questions Related to the Suspension of Certain U.S. Sanctions with Respect to Venezuela on October 18, 2023" (November 16, 2023), available here.

3 U.S. Department of the Treasury, "Following Terrorist Attack on Israel, Treasury Sanctions Hamas Operatives and Financial Facilitators" (October 18, 2023), available here; U.S. Department of the Treasury, "United States and United Kingdom Take Coordinated Action Against Hamas Leaders and Financiers" (November 14, 2023), available here.

4 U.S. Department of the Treasury, "Possible Evasion of the Russian Oil Price Cap" (April 17, 2020), available here; U.S. Department of the Treasury, "Treasury Imposes Additional Price Cap-Related Sanctions" (December 1, 2023), available here; U.S. Department of the Treasury, "Treasury Sanctions Additional Maritime Companies, Vessels Transporting Oil Sold Above the Coalition Price Cap" (November 16, 2023), available here U.S. Department of the Treasury, "Treasury Sanctions Entities for Transporting Oil Sold Above the Coalition Price Cap to Restrict Russia's War Machine" (October 12, 2023), available here ; *See also* U.S. Department of the Treasury, "The Price cap on Russian Oil: A Progress Report" (May 18, 2023), available here.

5 U.S. Department of the Treasury, " One Year On: The OFAC-OFSI Enhanced Partnership" (November 15, 2023), available here.

6 U.S. Department of the Treasury, "United States and United Kingdom Take Coordinated Action Against Hamas Leaders and Financiers" (November 14, 2023), available here.

7 Reuters, "Canada Imposes New Myanmar-related Sanctions in Coordination with US, UK" (October 31, 2023), available here.

Enforcement Against Non-U.S. Entities and Expanding Jurisdictional Reach

U.S. sanctions also continue to extend extraterritorially to non-U.S. entities, including in the digital asset realm. Indeed, of the 17 civil penalties imposed by OFAC in 2023, roughly half involved apparent violations by non-U.S. entities, including a $968,618,825 settlement with virtual currency exchange Binance Holdings, Ltd. in conjunction with the U.S. Department of Justice, the Financial Crimes Enforcement Network and the Commodity Futures Trading Commission.[8]

The U.S. government has also recently sought to expand OFAC's statutory authorities to impose secondary sanctions against non-U.S. financial institutions and other entities on multiple fronts.

The U.S. government has also recently sought to expand OFAC's statutory authorities to impose secondary sanctions against non-U.S. financial institutions and other entities on multiple fronts. For example, on November 28, 2023, the U.S. Treasury Department requested that Congress expand its authority to impose secondary sanctions on digital asset service providers engaged in dealings with terrorist groups and other illicit actors outside of U.S. jurisdiction.[9] In turn, on December 11, 2023, a bipartisan group of senators introduced a bill directing the U.S. President to impose so-called "mandatory" sanctions against foreign financial institutions and digital asset service providers that knowingly facilitate any significant financial transaction with sanctioned terrorist organizations.[10]

Similarly, on December 22, 2023, the Biden Administration issued an executive order authorizing the imposition of secondary sanctions against foreign financial institutions for engaging in significant transactions on behalf of certain sanctioned parties or otherwise involving Russia's military-industrial base, including transactions relating to certain identified items.[11]

As political transitions bleed into potential changes in sanctions policies, boards should expect continued efforts among the United States and its partners and allies to cooperate on sanctions issues where interests align.

Looking Ahead

Entering 2024, boards of directors should prepare for another dynamic year with elections scheduled in over 50 countries representing more than half the global population. As political transitions bleed into potential changes in sanctions policies, boards should expect continued efforts among the United States and its partners and allies to cooperate on sanctions issues where interests align.[12] U.S. sanctions against Russia, in coordination with U.S. partners and allies, are expected to further expand, in particular against the Russian military-industrial complex, Kremlin-linked elites and sanctions and export control evasion networks.[13] Companies with activities relating to Venezuela or its

8 For further discussion, *see* 2023 Year-in-Review: Developments and Trends in White Collar Enforcement Litigation.

9 U.S. Department of the Treasury, "Remarks by Deputy Secretary of the Treasury Wally Adeyemo at the 2023 Blockchain Association's Policy Summit" (November 29, 2023), available here.

10 U.S. Senator for Rhode Island, Jack Reed, "Reed Helps Lead Bipartisan Effort to Enforce Sanctions & Crackdown on Illicit Crypto Terrorist Financing" (December 11, 2023), available here.

11 U.S. Department of the Treasury, "Statement from Secretary Yellen on President Biden's Executive Order Taking Additional Steps with Respect to Russia's Harmful Activities" (December 22, 2023), available here.

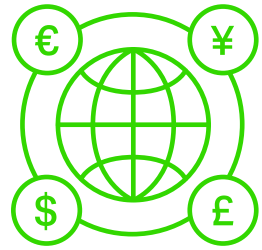
12 U.S. Department of Treasury, "U.S. and EU Sanctions Teams Enhance Bilateral Partnership" (May 16, 2023), available here.

13 U.S. Department of the Treasury, "With Wide-Ranging New Sanctions, Treasury Targets Russian Military-Linked Elites and Industrial Base" (September 14, 2023), available here ; U.S. Secretary of State, Antony Blinken, "Taking Additional Sweeping Measures Against Russia" (November 2, 2023), available here; U.S. Secretary of State, Antony Blinken, "Taking Additional Sweeping Measures Against Russia" (November 2, 2023), available here; U.S. Department of the Treasury, "Department of Commerce, Department of the Treasury, and Department of Justice Tri-Seal Compliance Note" (March 2, 2023), available here.

energy sector should also closely monitor the political situation in Venezuela for potential implications on U.S. sanctions policy.

Lastly, boards of directors should be cognizant of the willingness of OFAC to exercise its broad jurisdictional powers, including with respect to U.S. financial institutions and service providers in facilitating international and digital-asset transactions. Irrespective of the outcome of the 2024 U.S. presidential election, the U.S. government will likely continue to wield the threat of secondary sanctions and apply sanctions enforcement broadly with respect to key areas of focus, such as digital assets.

FDI Review Regimes are Well-Established and Active; Outbound Investment Regimes are on the Horizon



Chase D. Kaniecki
Partner
Washington, D.C.
ckaniecki@cgsh.com

Samuel H. Chang
Associate
Washington, D.C.
sachang@cgsh.com

William S. Dawley
Associate
Washington, D.C.
wdawley@cgsh.com

B.J. Altvater
Associate
Washington, D.C.
baltvater@cgsh.com

In 2024, boards of directors face a well-established, complex and active global foreign direct investment (FDI) landscape in which transactions will regularly trigger multijurisdictional FDI filing and approval processes. This is the case not only with respect to well-known FDI review regimes such as the Committee on Foreign Investment in the United States (CFIUS), but also with newly established, modified, and/or expanded non-U.S. FDI review regimes, particularly in Europe. Indeed, as governments around the world have become increasingly empowered and willing to scrutinize, and in some cases prevent, transactions they deem objectionable, FDI approvals have become a significant regulatory issue for many cross-border transactions.

Moreover, while existing FDI review regimes focus on inbound investment (i.e., investment by foreign persons into the relevant jurisdiction), the United States is developing, and the European Union is considering, restrictions and prohibitions on certain outbound investments (i.e., investments by U.S. and EU persons outside of the United States and European Union). If adopted, such restrictions and prohibitions could complicate, disrupt and in some cases prohibit certain cross-border investments by U.S. or EU investors involving so-called “countries of concern.”

FDI review analyses are often subjective and driven by factors of interest to each particular country, including factors that may not be known to the transacting parties.

Recent FDI Developments

Most existing FDI review regimes focus on national security- or national interest-related concerns, such as (1) access to defense-related or otherwise sensitive export controlled technology or other information (e.g., personal data) and (2) potential disruption to essential public services, supply chains or critical or sensitive infrastructure. However, the jurisdictional thresholds, review timelines and substantive tests vary by country, sometimes significantly. Moreover, FDI review analyses are often subjective and driven by factors of interest to each particular country, including factors that may not be known to the transacting parties. To further complicate matters, FDI review authorities have broad discretion to assert jurisdiction over transactions and to determine what does or does not qualify as a relevant concern. All of these factors combine to provide unique challenges to cross-border investors.

CFIUS appears willing to use its enforcement authorities – which can result in the imposition of significant penalties – to ensure that (1) mandatory CFIUS filings are made and (2) CFIUS mitigation agreements are fully complied with.

We highlight below major 2023 developments relating to certain key FDI review regimes:

— **United States**. Although there were no changes to the laws or regulations underlying the CFIUS regime in 2023, CFIUS continues to be very active in reviewing transactions notified to it, inquiring about so-called "non-notified" transactions (i.e., transactions within the jurisdiction of CFIUS but that were not notified to CFIUS by the transacting parties), and imposing mitigation where it identifies national security concerns. CFIUS continues to remain interested in transactions that (1) involve Chinese investors, non-Chinese investors with significant ties to China or that otherwise have China-related touchpoints; (2) implicate the semiconductor industry; (3) involve U.S. businesses that provide products or services, directly or indirectly, to U.S. government customers; (4) involve U.S. businesses involved with artificial intelligence or similar emerging or other sensitive technologies; and (5) involve U.S. businesses that collect or maintain data from or about U.S. persons. In addition, consistent with guidance issued by the U.S. Department of the Treasury in late 2022, CFIUS appears willing to use its enforcement authorities – which can result in the imposition of significant penalties – to ensure that (1) mandatory CFIUS filings are made and (2) CFIUS mitigation agreements are fully complied with.[1]

— **European Union**. Following the European Union's 2021 adoption of its FDI regulation, which laid out a common framework for FDI reviews by, and created an information sharing and cooperation mechanism between, EU member states, there have been significant FDI developments throughout the European Union. As of the date of this publication, 23 out of 27 EU member states have FDI review regimes and the other four EU member states are adopting, or are expected to adopt, FDI review regimes in 2024. Among other developments, in 2023:

- **Belgium.** The Belgian FDI review regime – which includes mandatory and suspensory notification requirements – went into effect on July 1, 2023.[2]

- **Ireland**. The new Irish FDI legislation was signed into law in 2023 and the Irish FDI review regime is expected to go into effect during the first half of 2024.

- **Luxembourg**. The Luxembourg FDI review regime – which includes mandatory notification requirements – went into effect on September 1, 2023.[3]

---

1 For additional details, see our October 2022 blog post available here.

2 For additional details, see our July 2023 alert memo available here.

3 For additional details, see our September 2023 blog post here.

- **The Netherlands**. The Dutch FDI review regime – which includes mandatory and suspensory notification requirements – went into effect on June 1, 2023.[4]

— **United Kingdom.** The UK FDI review regime has been in effect for approximately two years. In November 2023, the UK government opened a consultation regarding its FDI review regime, seeking stakeholder input on the first two years of experience under the regime and possible changes.

Under the proposed U.S. outbound investment regime, U.S. persons would be prohibited from making, or required to notify the U.S. government regarding, certain investments in entities engaged in certain activities relating to semiconductors and microelectronics, quantum information technologies and artificial intelligence involving "countries of concern."

Outbound Investment Regime Proposals

In August 2023, the Biden Administration issued a long-awaited executive order and accompanying rulemaking proposal setting forth the contours of an outbound investment regime targeting China. Under the proposed U.S. outbound investment regime, U.S. persons would be prohibited from making, or required to notify the U.S. government regarding, certain investments in entities engaged in certain activities relating to semiconductors and microelectronics, quantum information technologies and artificial intelligence involving "countries of concern" (presently limited to China, Hong Kong and Macau). Although previously referred to informally as "Reverse CFIUS" in industry circles, the proposed regime would not involve a case-by-case review of outbound investments. Instead, the proposed regime would require parties to determine whether a given transaction is prohibited, subject to notification or permissible without notification. There has been no guidance on when the final regulations for the proposed regime will be issued or when the proposed regime may take effect.[5]

In parallel, in August 2023, the European Commission issued a communication that included discussion of potential outbound investment rules that would have a similar scope as the proposed U.S. outbound investment regime (i.e., the rules would target China and be focused on investments in areas such as quantum computing, advanced semiconductors and artificial intelligence). However, as of the date of this publication, there has been no formal proposal regarding an EU outbound investment regime.

The proposed U.S. outbound investment regime and a potential EU outbound investment regime would be aimed at (1) limiting U.S. and EU support of certain industries in China and (2) preventing the transfer of sensitive technology or intellectual property from U.S. and/or EU companies to China. Although there is still significant uncertainty regarding the proposed/potential outbound investment regimes, there appears to be significant support for such regimes in the United States and Europe. Such regimes, if adopted, could significantly disrupt U.S. and EU investment in certain Chinese industries.

Boards of directors should ensure that they are directing their management teams to conduct thorough due diligence and analysis in connection with cross-border transactions, especially transactions involving companies involved in sensitive sectors or activities.

[4] For additional details, see our July 2023 alert memo available here.

[5] For additional details, see our August 2023 blog post available here.

Given the consequences that existing FDI review regimes can have for cross-border transactions, and the potential implications of outbound investment regimes, boards of directors would be well advised to stay up-to-date on related developments in key jurisdictions, particularly in North America, Europe, and Asia.[6] In addition, boards of directors should ensure that they are directing their management teams to conduct thorough due diligence and analysis in connection with cross-border transactions, especially transactions involving companies involved in sensitive sectors or activities (i.e., companies in the semiconductor or artificial intelligence industries and companies that collect and maintain sensitive (including personal) information) or with government (particularly defense or security-related) relationships, think about how FDI filing and clearance timelines overlap with other regulatory processes (including, for example, merger control/antitrust filings), and consider risk allocation when identifying closing conditions and agreeing to regulatory efforts provisions.

[6] As of the date of this publication, most countries in Central and South America and Africa generally have no or very limited FDI review regimes, although those countries may separately limit or prohibit foreign investment or ownership in certain industries or companies. However, Mexico is considering the creation of an FDI review regime. For additional details, see our December 2023 blog post available here.

Privacy and Data Protection Compliance Will Become More Fragmented in 2024

Daniel Ilan
Partner
New York
dilan@cgsh.com

Marcela Robledo
Partner
Bay Area
mrobledo@cgsh.com

Melissa Faragasso
Associate
New York
mfaragasso@cgsh.com

Christine D'Alessandro
Associate
New York
cdalessandro@cgsh.com

Continuing global trends to protect consumer privacy and rein in the exploitation of personal data by organizations, 2023 saw an explosion of comprehensive privacy laws, amendments to existing laws and a proliferation of targeted regulations around the world.

In the U.S., given the federal government's continued inability to enact a comprehensive federal privacy law, several U.S. states followed the path first paved by California and enacted comprehensive privacy legislation. 2024 will likely follow a similar trend with additional states aiming to pass comprehensive legislation, and will also see the laws passed in Texas, Florida, Montana and Oregon come into effect.[1] In addition to these new laws, regulatory bodies in California, Colorado and Connecticut took steps to build upon previously enacted privacy legislation with the promulgation of new regulations and amendments to enhance existing statutory requirements. In 2024, practices such as data mapping will remain critical for businesses to determine which state laws may apply to their processing activities based on what data they collect and how it is used. Companies will also need to be prepared to respond to consumer requests from additional states and, in many cases, to recognize universal opt-out mechanisms.

At the federal and state level, agencies remained focused on enhanced cybersecurity protections and enforcement of rules to safeguard consumer

[1] While many of these laws were constructed using similar models, there are key differences among the laws, particularly with respect to applicability thresholds. For a comparison of the applicability thresholds under various of the new state privacy laws, please see our June 2023 blog post available here.

nonpublic information. For example, the Federal Trade Commission and New York Department of Financial Services enacted new amendments and rules relating to cybersecurity as is discussed further below. It is expected that 2024 will bring continued enforcement from both the FTC and state attorneys general.

Similarly, privacy remained a legislative and regulatory priority abroad in 2023. For example, this summer, the European Commission officially adopted its adequacy decision for the new EU-U.S. Data Privacy Framework (the Framework), which replaces the invalidated Privacy Shield and is the latest mechanism designed to facilitate the transfer of personal data between the from the EU to U.S. organizations participating in the Framework.[2] As with the Privacy Shield and, prior to that, the Safe Harbor, the Framework has already been challenged, and companies will need to decide whether it makes sense to be certified as part of the Framework. In the UK and India, new comprehensive privacy legislation was advanced to update and in some ways replace existing privacy regimes in each country, and new privacy legislation or regulation is expected in Indonesia and Brazil, and other nations will likely follow.

Below, we have provided high level summaries of these developments, as well as provided links to more comprehensive discussions where available.

Not being able to rely on a comprehensive privacy law, companies will need to navigate the myriad of state laws to determine their applicability and the potential differing requirements for each one. This was an issue in 2023 but will be even more acute in 2024 given the amount of state laws that are coming into effect.

[2] For a discussion of the EU-U.S. Data Privacy Framework, please see below and our August 2023 blog post available here.

U.S. Privacy Developments

— **Eight States Pass Comprehensive Privacy Legislation**. Over the course of 2023, eight states—Florida, Texas and Oregon (each effective July 1, 2024), Montana (effective October 1, 2024), Iowa (effective January 1, 2025), Delaware (effective January 1, 2025), Tennessee (effective July 1, 2025) and Indiana (effective January 1, 2026)—passed consumer privacy laws, adding to the growing list of states with comprehensive privacy legislation alongside California, Virginia, Colorado, Connecticut and Utah. Many of the laws passed this year generally share commonalities with the previously enacted state privacy frameworks, outlining certain standards for data processors and controllers (*e.g.*, data minimization and purpose limitation standards), requiring notices to consumers about specific data-related practices and giving consumers specific rights with respect to their data, among other provisions.[3] With five comprehensive privacy acts now signed into law and in effect, eight states with signed privacy laws that will come into effect in 2024-2026, and at least ten other states with bills being submitted through the state legislatures, the landscape for covered businesses is expected to grow even more complicated as these laws take effect or proceed through the legislative process. While there are certain similarities across the acts, each has a unique character that will require careful consideration by impacted businesses and will require sufficient resources and investment to ensure continued compliance. Not being able to rely on a comprehensive privacy law, companies will need to navigate the myriad of state laws to determine their applicability and the potential differing requirements for each one. This was an issue in 2023 but will be even more acute in 2024 given the amount of state laws that are coming into effect.

[3] Uniquely, unlike the other states which passed comprehensive privacy legislation, Florida's privacy law introduces a more narrow scope and incorporates not only obligations on data controllers and processors related to the collection and processing of consumer personal data, but also measures specific to government-directed content moderation of social media and safeguards for the processing of children's data.

— **California Continues to Pioneer Privacy Legislation**. California regulators remained active in the privacy space in 2023, with the passage of new laws to address consumer privacy rights and advancement of regulations to guide compliance by covered entities. In March, the California Privacy Protection Agency (the CPPA), the newly created state agency tasked with interpreting and enforcing the California Consumer Privacy Act (CCPA) pursuant to the amendments set forth under the California Privacy Rights Act (CPRA), announced finalized CCPA regulations (the Regulations).[4] Originally set to take effect with the CPRA amendments on July 1, after legal challenges brought by the California Chamber of Commerce,[5] the Sacramento County Superior Court enjoined enforcement of the regulations until March 29, 2024.

Undeterred by the court's delay, the CPPA continued to forge ahead with its rulemaking process, preparing and publishing draft proposals for future rulemaking packages with respect to the CPRA amendments' cybersecurity audit, risk assessment and automated decision making technology requirements.

Undeterred by the court's delay, the CPPA continued to forge ahead with its rulemaking process, preparing and publishing draft proposals for future rulemaking packages with respect to the CPRA amendments' cybersecurity audit, risk assessment and automated decision making technology requirements. Though these proposals have been discussed at various board meetings occurring during the latter half of 2023, the formal rulemaking process has yet to begin, and the draft proposals remain subject to ongoing CPPA review and revision. Finally, at its last board meeting, the CPPA also advanced a draft of proposed revisions to the Regulations for discussion purposes, with formal rulemaking yet to commence. Accordingly, formal drafts and eventually finalized regulations are not expected until well into 2024.

While the CPPA focused on its rulemaking processes, the California legislature worked in parallel to pass amendments to California's existing data broker law to enhance consumer deletion rights first provided under the CCPA. The amendments, referred to as the "California Delete Act," are intended to simplify the process by which consumers can request deletion of their personal data held by data brokers. Specifically the CPPA is tasked with, prior to January 2026, establishing an accessible deletion mechanism that allows a consumer, through a single verifiable consumer request, to simultaneously request that every California-registered data broker delete such consumer's personal information from their repositories and direct their associated service providers or contractors to do the same.[6]

— **Children's Privacy Rights Will Continue to be at the Forefront**. In the realm of children's privacy, the California Age-Appropriate Design Code (the Code), which was scheduled to take effect on July 1, 2024, may be delayed after a California federal court issued a preliminary injunction in September. The Code, which imposes heightened requirements on businesses that provide online products, services or features likely to be accessed by children, was challenged by NetChoice, LLC (NetChoice) on constitutional grounds under the First and Fourth

[4] At a high level, among other things, the Regulations (i) define select terms that were used, but not defined, in the CPRA; (ii) elaborate on the requirements for disclosures to consumers, including the formatting and placement of such notices; (iii) explain how to request and obtain consumer consent; (iv) revise the requirements related to information included in a company's privacy policy; (v) provide guidance with respect to opt-out, alternative opt-out and other data processing limitation links; (vi) set forth requirements related to the recognition of opt-out preference signals; and (iv) summarize contractual requirements for service providers, contractors, and third parties with whom business sell or share personal information.

[5] In its lawsuit filed against the CPPA, the Chamber of Commerce argued that due to the delay in finalizing the rulemaking package until eight months after the statutory deadline, the CPPA failed to provide businesses with a 12-month grace period to come into compliance as set forth under the statute.

[6] For a broader discussion of the California Delete Act, see our October 2023 blog post available here.

Amendments. Persuaded that certain of the Code's provisions were unlikely to pass constitutional muster as insufficiently tailored to advance the government's interest in protecting minors' wellbeing online, the District Court for the North District of California granted NetChoice's request for a preliminary injunction, holding that the Code's provisions would unlawfully target protected speech, including by forcing websites to impose barriers for children that would also likely impact adults given the difficulty of accurately estimating the age of a business's users, as required by the Code. The California Attorney General has since filed an appeal of the decision, which remains pending.

The Rules set forth technical specifications for universal opt-out mechanisms, including obligations on the Colorado Department of Law to maintain a list of universal opt-out mechanisms that meet the standards set forth in the Rules.

Also, the Federal Trade Commission on December 20, 2023 proposed a set of revisions to its rules implementing the Children's Online Privacy Protection Act (COPPA). The FTC proposal, which remains subject to a sixty day public notice and comment period, is aimed at strengthening COPPA's restrictions imposed on website operators' processing of children's personal information to account for the evolving technological landscape, particularly in light of advancements relating to the ed-tech sector, voice-enabled connected devices and general audience platforms that host third-party child-directed content[7].

— **Colorado Adopts Privacy Act Regulations**. In March, the Colorado Attorney General's Office finalized the Colorado Privacy Act Rules (the Rules), which supplement and enhance the requirements of the Colorado Privacy Act that came into effect on July 1.[8] Most notably, the Rules set forth technical specifications for universal opt-out mechanisms, including obligations on the Colorado Department of Law to maintain a list of universal opt-out mechanisms that meet the standards set forth in the Rules. In recent weeks, the Global Privacy Control (which businesses are also required to recognize pursuant to the CCPA) has been recognized by the Colorado Attorney General as the first valid universal opt-out mechanism with which controllers must comply.

— **Connecticut Amends Data Privacy Act**. In June, the Connecticut legislature amended the Connecticut Data Privacy Act (CTDPA), which took effect on July 1, broadening the scope of the CTPDA and providing enhanced protections for consumer health and children's data. While certain provisions of the amendments, including protections for consumer health data, came into effect simultaneously with the CTDPA, others will take effect in 2024.[9]

[7] For a broader discussion of the FTC revisions, see our January 2024 blog post available here.

[8] At a high level, the Rules include (i) enhanced privacy notice and disclosure requirements, including a requirement that controllers notify consumers of material changes to its privacy notice; (ii) a requirement that controllers keep records of consumer data rights requests for a minimum of twenty-four months; (iii) expanded requirements related to conducting and documenting data protection assessments; and (iv) a requirement to "refresh" consent for certain types of processing when a consumer has not interacted with the controller in the past twenty-four months. Finally, the Rules also address the use of dark patterns and provide a set of principles to consider when designing user interfaces.

[9] Examples of such amendments include (i) requirements that social media platforms institute procedures to allow and honor requests of individuals under eighteen to unpublish and delete their social media accounts and (ii) with respect to controllers that provide an online service, product or feature to individuals under the age of eighteen (a) obligations to conduct data protection impact assessments to assess, and use reasonable care to avoid, heightened risks of harm to minors arising therefrom and (b) prohibitions on (1) the processing of such individual's data for the purposes of targeted advertising, personal data sales or certain types of profiling, (2) the collection of such individual's precise geolocation data and (3) using any system design feature to significantly increase, sustain or extend any such individual's use of such online service, product or feature.

U.S. Cybersecurity Developments

— **NY Department of Financial Services Finalizes Amendments to its Cybersecurity Regulation**. In November, the New York Department of Financial Services (the Agency) announced finalized amendments to its Cybersecurity Regulation (the Amendments), which contained significant revisions designed to mandate preventative measures to address common attack vectors and enhance cybersecurity governance.[10] Updates to existing reporting requirements (*e.g.*, the cybersecurity event notification and annual compliance certification obligations) went into effect on December 1; however, for most provisions, entities will have 180 days (*i.e.*, until April of 2024) to comply, while certain other provisions (such as those related to incident response planning, governance and encryption) will have different transitional periods for compliance as further set forth in the Amendments.[11]

— **FTC Finalizes Amendments to GLBA Safeguards Rule**. In October, the Federal Trade Commission (the FTC) finalized its supplemental revisions to the 2021 amendments to its implementation of the Gramm Leach Bliley Act Safeguards Rule (the Amended Safeguards Rule). The supplemental revisions to the Amended Safeguards Rule, which are expected to take effect in May of 2024, will require covered non-banking financial institutions—*e.g.*, automobile dealerships, mortgage brokers, payday lenders, retailers that issue credit cards—to report to the FTC those "notification events," which are events involving the unauthorized acquisition of unencrypted customer information impacting at least 500 customers. Such reports should be done as soon as possible, but in any event no later than thirty days after discovery.[12]

The supplemental revisions to the Amended Safeguards Rule will require covered non-banking financial institutions to report to the FTC those "notification events," which are events involving the unauthorized acquisition of unencrypted customer information impacting at least 500 customers.

International Developments

— **EU-US Data Privacy Framework Adopted**. In July, the European Commission adopted its adequacy decision for the new EU-U.S. Data Privacy Framework, concluding that the U.S. ensures an adequate level of protection for personal data transferred from the EU to U.S. organizations participating in the Framework. This allows EU organizations to freely transfer personal data that is subject to the GDPR to those organizations in the U.S. who have decided to enroll in the Framework.

More specifically, the Framework is based on a system of certification. EU data exporters will only benefit from this adequacy decision if they are transferring data to U.S. organizations certified under the Framework. Therefore, any data transfers to other U.S. organizations not certified will still need to be subject to additional appropriate safeguards (*e.g.*, standard contractual clauses or binding corporate rules) or will need to rely on a derogation under the GDPR.

[10] Specifically, the Amendments impose (i) heightened compliance obligations for "Class A Companies" or larger organizations that meet certain revenue and size thresholds, including requirements to conduct annual, independent audits of its cybersecurity program, monitor user privileged access activity and implement endpoint detection and response solutions, (ii) mandatory revisions to internal cybersecurity policies and procedures, including access control, business continuity and incident response plans and policies, which now must be approved annually approved by the covered entity's senior governing body, (iii) enhanced governance requirements, including increased board oversight; (iv) enhanced extortion payment reporting requirements, (v) alternative "acknowledgement of noncompliance" filings for entities that cannot certify compliance to the Agency and (vi) revisions to Agency enforcement and penalties.

[11] For a detailed discussion of the Amendments, see our November 2023 blog post available here.

[12] For a detailed discussion of the Amended Safeguards Rule, see our Novebmer 2023 blog post available here.

Underpinning the Framework is a set of privacy principles issued by the U.S. Department of Commerce—the 'EU-U.S. Data Privacy Framework Principles'—with which the certified U.S. organizations will need to comply. Additionally, in order to be eligible for certification under the Framework, U.S. organizations must be subject to the investigatory and enforcement powers of the FTC or the U.S. Department of Transportation.

Certain critics and privacy advocacy groups have publicly contested the validity of this adequacy decision, which has already been challenged before the Court of Justice of the European Union. A decision on such challenge is not expected until 2025.

Multi-national organizations that have EU operations will also need to take care when considering the extent to which they will need to revise their data protection governance framework to fully take advantage of the changes proposed by the Bill.

— **The UK Data Protection and Digital Information Bill**. In November, the UK government introduced a number of amendments to the Data Protection and Digital Information (No. 2) Bill (the Bill), which proposes to update the current UK data protection regime.[13] The UK government hopes that the Bill will reduce administrative and financial burdens on organizations, provide them with greater flexibility on how to comply with certain aspects of the UK data protection law, and increase public and business confidence in AI technologies. The Bill is also intended, among other things, to cut down on "user consent" pop-ups and banners.

Overall the Bill does not intend radically to change the core principles, concepts and obligations of organizations under the current UK data protection regime, which is currently largely aligned with the corresponding EU regime. However, if the Bill is passed into legislation, it will create a degree of uncertainty, along with the potential for increased compliance costs and risks for affected businesses. Moreover, multi-national organizations that have EU operations will also need to take care when considering the extent to which they will need to revise their data protection governance framework to fully take advantage of the changes proposed by the Bill.

Furthermore, the EU currently recognizes the UK as an "adequate" jurisdiction, which means that companies can transfer EU data to the UK without putting in place any additional safeguards such as entering into EU-approved standard contractual clauses. Whether or not the Bill will have any impact on the UK adequacy's status is still not clear, but the process is largely out of the control of the UK government. While one could argue that the UK data protection regime will remain the closest aligned with the EU data protection regime even after the Bill is passed, the final decision will ultimately rest with the EU.

— **India Introduces Comprehensive Privacy Law**. In August, India passed the long-awaited Digital Personal Data Protection Act, 2023 (the DPDPA) into law.[14] While the DPDPA includes many familiar elements, such as (i) free, purpose-specific, informed consent, based on transparent notice and (ii) technical and organizational measures and appropriate security practices to secure data—it has several distinctive aspects, including a flat definition of what constitutes personal data, a remarkably consent centric regime (leaving private entities with few other lawful bases for processing), a requirement to demonstrate necessity even where consent has been obtained,

[13] The Bill and relevant documentation, including the Bill's Explanatory Notes, can be found here.

[14] For a comparison of the DPDPA with the EU and UK General Data Protection Regulation, as well as the CCPA, see our January 2024 blog post available here.

statutory data retention thresholds and a potential "black list" of jurisdictions to which transfers may be restricted. Many of the DPDPA's provisions remain subject to further refinement once the Central Government begins its rulemaking procedures in the coming weeks; however, enforcement is not expected as an effective date has not yet been established and there is no concrete timeline for implementation.

Hot Tax Topics for Multinational Groups, in the US, the EU and Beyond

Jason R. Factor
Partner
New York
jfactor@cgsh.com

Richard Sultman
Partner
London
rsultman@cgsh.com

Vania Petrella
Partner
Rome
vpetrella@cgsh.com

Anne-Sophie Coustel
Partner
Paris
acoustel@cgsh.com

Jens Hafemann
Counsel
Frankfurt
jhafemann@cgsh.com

Benjamin Boisanté
Senior Attorney
Paris
bboisante@cgsh.com

Gianluca Russo
Senior Attorney
Milan
grusso@cgsh.com

Impact of "Pillar Two" Global Minimum Taxation

The push for global tax reform will continue to have a significant impact on large multinational groups in 2024. Since broad international consensus was reached through the Organisation for Economic Co-operation and Development (OECD) in 2021 on the principles of a "two-pillar solution" to tax challenges arising from the digitalization of the world economy, many of the countries that support the plan (of which there are now over 140) have rushed through legislation to implement the second pillar (a global minimum rate of effective taxation) by the end of 2023. Many of the new "Pillar Two" rules will accordingly apply for the first time in 2024, and companies should be sure they understand both the overall global impact and how local nuances create differences between jurisdictions.

Pillar Two aims at ensuring that large multinationals pay a minimum 15% effective tax on their worldwide income (as determined on a jurisdiction by jurisdiction basis), wherever they are headquartered or have their business operations. The rules will apply to multinational groups with €750 million or more in consolidated revenues, although not sovereign, nonprofit or charitable entities, or pension, investment and real estate funds. There is also an exclusion for international shipping income. Other limitations include a *de minimis* exclusion for jurisdictions where revenues and profits are low, and a substance carve out that excludes certain amounts of income based on the carrying value of tangible assets and payroll.

The main tool to achieve the minimum tax is a global anti-base erosion regime consisting of two components: an income inclusion rule (IIR) and an undertaxed payments rule (UTPR). The objective is for in-scope multinational groups to pay a top up tax on the difference between the minimum 15% tax rate and their effective tax rate per jurisdiction, if lower. The IIR will generally charge the top up tax in the jurisdiction of the ultimate parent company. The UTPR would function as a backstop if IIR rules do not pick up all of the group's low-taxed income – it would require adjustments (for example, by denying deductions) to increase tax levels in subsidiary jurisdictions.

In many cases, these two rules will be supplemented by a locally enacted qualified domestic minimum top-up tax (QDMTT). A QDMTT is a domestic minimum tax that applies to local constituent entities of in-scope multinational groups, topping up local taxes to the globally agreed minimum effective 15%. The attraction of a QDMTT to a local jurisdiction is that it should allow that jurisdiction (rather than the parent company jurisdiction or another group company jurisdiction) to collect the relevant top-up tax in relation to the otherwise low-taxed local income.

Regarding implementation, a Pillar Two Directive required Member States of the EU to transpose the global minimum tax rules into domestic law by December 31, 2023, with the IIR being effective on or after December 31, 2023 and the UTPR becoming effective on or after December 31, 2024. Most EU countries (including Germany, France and Italy) enacted their implementing legislation within that timeframe, as did the UK. Germany, France, Italy and the UK also all enacted a QDMTT. Many other countries outside the EU and the UK (including Australia, Japan and Canada) have either enacted Pillar Two legislation or are in the process of enacting their legislation.

Whether all the local rules will fit together remains to be seen, and many practical impacts of the new regime will continue to unfold in 2024 and beyond.

Whether all the local rules will fit together remains to be seen, and many practical impacts of the new regime will continue to unfold in 2024 and beyond. Consequences could be significant – ranging from increases in tax (the OECD recently estimated an increase in annual worldwide corporate income tax revenue of between $155 billion and $192 billion) and tax compliance, to commercial considerations and risk allocation for M&A transactions.

Certain major jurisdictions, like the US and China, have not introduced their legislation, even though they signed up to Pillar Two. Particular challenges present themselves in the US. The Biden administration has been one of the most forceful proponents of Pillar Two but 2021 ended with a failure to get Congress to enact the Build Back Better Act, which would have brought US tax law into compliance with Pillar Two. Thus, the United States still applies international tax rules (known as Global Intangible Low-Taxed Income (GILTI) and Base Erosion and Anti-Abuse Tax (BEAT)) that are not in line with Pillar Two's IIR and UTPR. The practical implications of this mismatch remain unclear, but could result in US multinationals being taxed multiple times on the same income, tax compliance burdens, and the need for structural changes or other tax planning to mitigate potential adverse effects.

The final component to note about Pillar Two is the subject to tax rule (STTR). The STTR is a new double tax treaty rule that will allow developing countries to deny treaty benefits in respect of interest, royalties and certain other payments that are subject to corporate income tax at below 9% in the recipient country, in effect creating a right to tax the difference. A model treaty provision to give effect to the STTR was published by the OECD in October 2023 for those countries which choose to implement it.

Large multinational groups should consult with their tax counsel for further details on Pillar Two as well as on Pillar One (a slower-moving OECD proposal for the reallocation of taxable income of large multinational businesses to customer jurisdictions, even if the business has no or minimal physical presence there).

International Cross-Border Tax Audits

In 2023, tax authorities continued the trend of conducting large-scale tax audits and cross border proceedings across Europe, relying on broader access to information and new technological tools.

Exchange of information / anti-avoidance rules

The provisions of a new EU Directive referred to as "DAC7" impose new tax disclosure obligations on online platform operators (i.e., entities that contract with sellers to make an online marketplace available). DAC7 targets transactions implemented through online platforms and seeks to ensure efficient tracking of such transactions by requiring the platform operators to disclose personal and trade details of platform members (such as their name, country of residence, and identification number, if any). DAC7 became effective as of January 1, 2023. The first assessment of the findings under DAC7 should be available in the course of 2024 after tax authorities have processed the first batch of disclosures. Similar rules came into effect in the UK from January 1, 2024.

The Council of the EU also adopted a "DAC8" Directive in October 2023, supplementing DAC 7 and targeting transactions relating to crypto assets (not only including crypto currencies but also certain other tokens). This new Directive is expected to enter force as of January 1, 2026.

On top of these legislative advances, tax authorities have also benefited from more effective exchange of information between EU (and non-EU) countries. In addition to sharing of information, international tax collaborations have also taken the form of joint procedures in which local and foreign tax authorities have worked together to investigate cross-border tax planning schemes and arrangements. In some cases, this has led to foreign tax agents assisting in dawn raids launched by local authorities. Companies should expect this kind of cross-border cooperation to be more prevalent going forward.

Not all EU-level tax initiatives are having similar levels of success. The proposal for a third Anti-Tax Avoidance Directive (ATAD 3) which was intended to combat the use of 'shell' companies, still lacks consensus among Member States. The Business in Europe: Framework for Income Taxation (BEFIT) proposal, which contemplates the introduction of a common system to compute the tax base of corporate groups across the EU, is also facing difficulties.

In certain jurisdictions, the targeting of tax audits has become predominantly driven by information obtained and processed through data mining.

Use of AI tools for data processing

Tax authorities have made significant investments in AI tools in order to better analyze the voluminous amount of information obtained through the operation of automatic exchange of information rules, and to identify transactions for further investigation. Dedicated teams specializing in data mining have been set up by tax authorities. As a result of such efforts, in certain jurisdictions, the targeting of tax audits has become predominantly driven by information obtained and processed through data mining. This can be expected to have a significant impact on future tax audit and reassessment trends.

The strengthening of tax enforcement in the EU has also been coupled with more severe legal responses, including ad hoc penalties aimed at tackling specific behaviors (such as the enabling of tax evasion), and a wider criminalization of certain tax reassessments (such as reassessments following a failure to disclose facts, or the provision of misleading information, in relation to beneficial owners of income or gains).

Partnerships and Collaboration between Taxpayers and Tax Authorities

Counterbalancing more severe audit and enforcement policies, several initiatives have been taken by tax authorities across Europe to offer more legal certainty to taxpayers. While each of these initiatives are country specific, there is a general trend towards a more collaborative approach with compliant taxpayers.

The most elaborate versions of such initiatives take the form of partnerships entered into by taxpayers and tax authorities. Under such partnerships, taxpayers that have demonstrated past compliance with tax rules and that commit to be transparent with the tax authorities on an ongoing basis may benefit from more direct access to the tax authorities, allowing them, in certain circumstances and under certain conditions, to discuss in advance with the tax authorities uncertain tax positions and agree on a reporting position that is protected from challenge. Although these kinds of partnerships have generally been designed for larger groups, some jurisdictions have also implemented simplified versions for the benefit of small or medium sized entities.

Lighter-touch versions of these initiatives provide benefits for cooperative taxpayers that include reinforcement of taxpayers' rights and the introduction of new remediation processes to correct mistakes or omissions.

Office Locations

Abu Dhabi
Al Sila Tower, 27th Floor
Abu Dhabi Global Market Square
Al Maryah Island, PO Box 29920
Abu Dhabi, United Arab Emirates
T: +971 2 412 1700
F: +971 2 412 1899

Bay Area

Silicon Valley
1841 Page Mill Road
Suite 250
Palo Alto, CA 94304
T: +1 650 815 4100
F: +1 650 815 4199

San Francisco
650 California Street
Suite 2000
San Francisco, CA 94108
T: +1 415 796 4400
F: +1 415 796 4499

Beijing
Cleary Gottlieb Steen & Hamilton LLP
45th Floor, Fortune Financial Center
5 Dong San Huan Zhong Lu
Chaoyang District
Beijing 100020, China
T: +86 10 5920 1000
F: +86 10 5879 3902

Brussels
Rue de la Loi 57
1040 Brussels, Belgium
T: +32 2 287 2000
F: +32 2 231 1661

Cologne
Theodor-Heuss-Ring 9
50668 Cologne, Germany
T: +49 221 80040 0
F: +49 221 80040 199

Frankfurt
Main Tower
Neue Mainzer Strasse 52
60311 Frankfurt am Main, Germany
T: +49 69 97103 0
F: +49 69 97103 199

Hong Kong
Cleary Gottlieb Steen & Hamilton
(Hong Kong)
Hysan Place, 37th Floor
500 Hennessy Road, Causeway Bay
Hong Kong
T: +852 2521 4122
F: +852 2845 9026

London
2 London Wall Place
London EC2Y 5AU, England
T: +44 20 7614 2200
F: +44 20 7600 1698

Milan
Via San Paolo 7
20121 Milan, Italy
T: +39 02 72 60 81
F: +39 02 86 98 44 40

New York
One Liberty Plaza
New York, NY 10006-1470
T: +1 212 225 2000
F: +1 212 225 3999

Paris
12, rue de Tilsitt
75008 Paris, France
T: +33 1 40 74 68 00
F: +33 1 40 74 68 88

Rome
Piazza di Spagna 15
00187 Rome, Italy
T: +39 06 69 52 21
F: +39 06 69 20 06 65

São Paulo
Cleary Gottlieb Steen & Hamilton
Consultores em Direito Estrangeiro
Rua Professor Atílio Innocenti, 165
São Paulo, SP Brazil 04538-000
T: +55 11 2196 7200
F: +55 11 2196 7299

Seoul
Cleary Gottlieb Steen & Hamilton LLP
Foreign Legal Consultant Office
19F, Ferrum Tower
19, Eulji-ro 5-gil, Jung-gu
Seoul 04539, Korea
T: +82 2 6353 8000
F: +82 2 6353 8099

Washington, D.C.
2112 Pennsylvania Avenue, NW
Washington, DC 20037-3229
T: +1 202 974 1500
F: +1 202 974 1999

CLEARY GOTTLIEB STEEN & HAMILTON LLP

clearygottlieb.com

23.1214.05_011924