CLEARY GOTTLIEB

Selected Issues for Boards of Directors in 2025

January 2025

Selected Issues for Boards of Directors in 2025

2025 promises to be another turbulent year for boards of directors. On the heels of a historically unprecedented election, companies are still ramping up compliance with the ambitious agenda of the outgoing administration while simultaneously bracing for the changes promised by the next one. Against that backdrop, colleagues from across Cleary's offices have zeroed-in on the impact of the issues that boards of directors and senior management of public companies have faced in the past year, as well as on what can be anticipated in the year to come.

The risks and opportunities created by AI remain top of mind and at the top of agendas for boards and their committees, as companies in every industry grapple with how to manage the use of these rapidly evolving technologies in their businesses. Executive security has likewise become a top priority across the board in light of recent events. 2024 was also a notable year for developments in U.S. tax, FDI and sanctions, Delaware corporate law, M&A, antitrust, cybersecurity and climate disclosure. European regulatory developments are continuing to drive board agendas in areas like tax, competition and capital markets.

With the social and political landscape in flux, companies must remain nimble as they prepare for widely disparate potential outcomes in everything from climate-related disclosure and executive benefits to antitrust and enforcement. We hope you will find this helpful as you navigate the year ahead. Review these topics by clicking on the headings listed below.

EDITORS

Francesca L. Odell

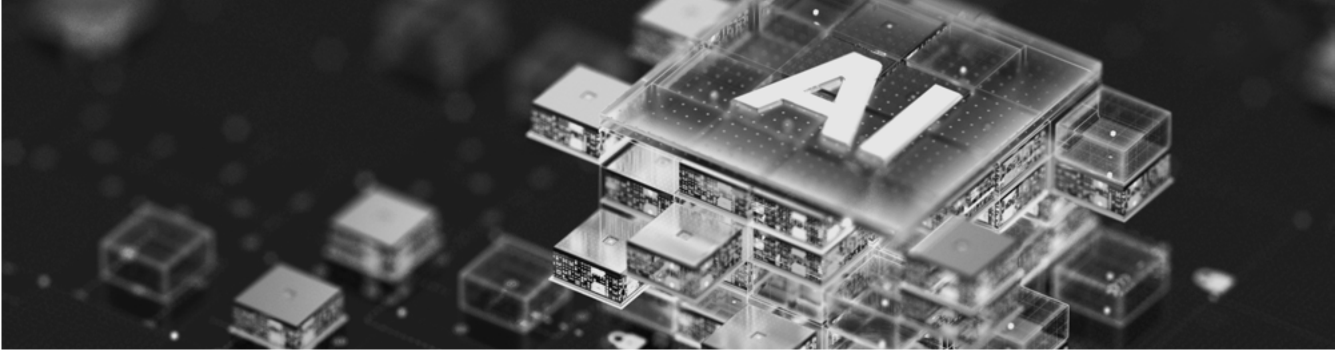
Helena K. Grannis

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



Effective Board Oversight as AI Evolves

Adam Fleisher
Partner
New York
afleisher@cgsh.com

Angela L. Dunning
Partner
Palo Alto
adunning@cgsh.com

Daniel Ilan
Partner
New York
dilan@cgsh.com

David Lopez
Partner
New York
dlopez@cgsh.com

Marcela Robledo
Partner
Bay Area
mrobledo@cgsh.com

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

Gaia Shen
Associate
London
gshen@cgsh.com

Natalie Curry
Associate
New York
ncurry@cgsh.com

Samuel Blankenship
Associate
Bay Area
sblankenship@cgsh.com

Jinhyun Kwon
Law Clerk
New York
jkwon@cgsh.com

Kimberly Bittinger
Law Clerk
Silicon Valley
kbittinger@cgsh.com

Deployment of generative AI expanded rapidly across many industries in 2024, leading to broadly increased productivity, return on investment and other benefits. At the same time, AI was also a focus for lawmakers, regulators and courts. There are currently 27 active generative AI litigation cases in the U.S., nearly all of which involve copyright claims. Numerous state legislatures have mulled AI regulation, and Colorado became the first and only state thus far to pass a law creating a broad set of obligations for certain developers and deployers of AI.

Though Congress has yet to seriously engage with AI legislation, the SEC and the FTC have been using existing laws to bring AI-related enforcement actions. Numerous other federal agencies have hinted at potential regulation of AI,[1] but the future of U.S. AI regulation is uncertain given the new administration and upcoming turnover in regulatory leadership. Meanwhile, the EU's Regulation No. 1689 (the EU AI Act) entered into force after three years of legislative debate.[2]

As the SEC steps up its enforcement against "AI washing"—making false or misleading claims about the use of AI in one's business—it remains critical for boards of directors to manage AI risks with an in-depth understanding of how AI is used in their businesses.[3]

[1] Various federal government agencies issued a Joint Statement on Enforcement of Civil Rights, Fair Competition, Consumer Protection, and Equal Opportunity Laws in Automated Systems, available here. The Examination Division of the SEC named AI as a priority in its FY2025 Examination Priorities, available here. FSOC cohosted a conference on AI with the Brookings Institution, as described in its press release, available here.

[2] Our previous coverage of the EU AI Act can be found in our blog posts available here and here.

[3] *See*, *e.g.*, Bloomberg Law, "AI-Washing Enforcement Crackdown Set to Survive Trump Rollbacks" (November 25, 2024), available here.

As the SEC steps up its enforcement against "AI washing"—making false or misleading claims about the use of AI in one's business—it remains critical for boards of directors to manage AI risks with an in-depth understanding of how AI is used in their businesses.

The Open Questions in U.S. Generative AI Copyright Litigation

Overview of AI Copyright Litigation

Whether training AI on copyrighted works constitutes fair use is a central issue in all 27 of the active generative AI cases. Under section 107 of the U.S. Copyright Act, the fair use of a copyrighted work, including for such purposes as criticism, commentary, news reporting, research or scholarship, is not copyright infringement. Courts consider four factors in determining whether a particular use is fair: (1) the purpose and character of the use, (2) the nature of the copyrighted work, (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole and (4) the effect of the use upon the potential market for or value of the copyrighted work. The primary inquiry is whether the challenged use is transformative, serving a different purpose or function from the original, or merely usurps the market for the original by reproducing it.

The first court to reach a decision on fair use in the context of an AI-augmented platform will likely be *Thomson Reuters Enterprise Center GmbH v. ROSS Intelligence Inc.*[4] In May 2020, Thomson Reuters sued ROSS Intelligence for allegedly copying headnotes from Westlaw, Thomson Reuter's legal research platform, to train its AI-based legal research platform. ROSS argues that it made fair use of the Westlaw material, while Thomson Reuters argues that ROSS used content from Westlaw to build a directly competing platform without

[4] 1:20-cv-00613 (D. Del. 2020).

its authorization. In December 2024, the court held a lengthy hearing on the parties' competing fair use positions at summary judgment, but no decision has yet been issued. If fair use cannot be resolved at summary judgment and the case proceeds to trial in May 2025, it will be the first AI copyright case to do so. Although the technology at issue in this case involves more traditional machine learning algorithms, it is being closely watched by litigants in the generative AI cases.

The first generative AI class action to reach summary judgment on fair use will almost certainly be *Kadrey et al. v. Meta Platforms, Inc.*[5] In this putative class action, a group of authors allege that Meta trained its Llama large language models on the text of their books without authorization. There are no allegations that the Llama models have been used to generate content resembling plaintiffs' books. Rather, the theory is strictly that using the books for training constitutes copyright infringement. Summary judgment on fair use is set to be heard in May 2025. Decisions in *Kadrey* have already proven influential in narrowing the claims asserted in AI litigation across the country,[6] and the court's ruling on fair use may do the same.

A fair use decision is also expected soon in *Concord Music Group et al. v. Anthropic PBC*.[7] There, dozens of music publishers allege that Anthropic infringed their rights by using copyrighted song lyrics to train Claude, Anthropic's large language model.[8] To date, this case is the only generative AI copyright case in which the plaintiffs have sought preliminary injunctive relief. In opposition to the motion, Anthropic asserts that Concord cannot establish irreparable harm, that fair use makes success on the merits unlikely and that a decision on fair use before discovery would be premature. The motion for preliminary injunction has been fully briefed and argued, and a decision is expected in early 2025.

In addition to cases focused on AI training, a number of cases assert direct (as opposed to class) actions based on allegedly infringing outputs. In *The New York Times Co. v. Microsoft Corp. et al.*,[9] for example, the New York Times sued OpenAI, alleging that ChatGPT can replicate the exact content of articles otherwise available only behind a paywall. OpenAI claims the plaintiffs engineered the chat prompts to obtain the allegedly infringing outputs in a manner that does not emulate real-world use.

Andersen, et al. v. Stability AI Ltd., et al,[10] a putative class action by a number of visual artists against several leading generative AI image and video developers such as Midjourney, presents a question of first impression: whether artists can claim a generative AI model infringes their trade dress. The artists claim that Midjourney should be held vicariously liable for trade dress infringement when Midjourney tools are used to create outputs that plaintiffs allege replicate their art styles. This novel claim tests the boundaries of trademark protection for "style," to which no copyright protection attaches, and will proceed to discovery and summary judgment along with the training-based copyright claim.

Regulatory Guidance on Copyright & AI

The courts will have final word on the fair use question, but the U.S. Copyright Office has promised further guidance on a number of other intellectual property issues, including the copyrightability of works created using generative AI, fair use in training AI, licensing considerations and allocation of potential liability between AI developers and users. The first installment of this guidance—on the use of digital technology to replicate an individual's voice or appearance—was released in July 2024.[11]

5 3:23-cv-03417 (N.D. Cal. 2023).

6 For additional discussion on earlier decisions in *Kadrey*, see our February 2024 blog post available here.

7 5:24-cv-03811 (N.D. Cal. 2024).

8 For additional discussion of the *Concord* case, see our June 2024 blog post available here.

9 1:23-cv-11195 (S.D.N.Y. 2023).

10 3:23-cv-00201 (N.D. Cal. 2023).

11 *See* U.S. Copyright Office, "Copyright and Artificial Intelligence Part 1: Digital Replicas" (July 2024), available here.

Legislating AI in 2024

U.S. State Legislative Trends

While courts continue to grapple with novel AI copyright issues, state lawmakers are turning their attention to AI in a number of other contexts. For example, California, New York and other states have considered bills addressing discrimination by automated decision-making tools (ADMT). New York's state legislature has proposed several bills that would limit use of ADMT by state agencies and an "AI Bill of Rights" that would provide New York residents with certain protections against use of ADMT without human intervention.

Numerous state legislatures also considered bills pertaining to the use of AI in employment contexts. These bills focused on areas such as providing notice to employees or potential employees of AI usage, limiting AI employee monitoring and identifying bias in employment decision tools. In addition, many state lawmakers focused on consumer protection and transparency—specifically, making consumers aware they are interacting with AI. For example, Utah passed its AI Policy Act,[12] which requires entities to disclose that a consumer is interacting with generative AI upon consumer request, or without request if AI is used by the entity in certain regulated occupations. California Senate Bill No. 942, effective January 1, 2026, similarly aims to facilitate consumer awareness of AI usage by requiring persons who create generative AI systems with over one million monthly visitors or users (and that are publicly accessible within California) to make an AI detection tool available at no cost. Finally, California AB 2013, effective January 1, 2026, requires developers of generative AI to provide, on their website, a high-level summary of the datasets used in developing their system, including whether the system uses synthetic data generation.

[12] Utah's AI Policy Act can be found here.

The Colorado AI Act

Colorado Senate Bill 24-205 Concerning Consumer Protections in Interactions with Artificial Intelligence Systems (the Colorado AI Act) was passed on May 17, 2024 and became the first law in the U.S to create a broad set of obligations for developers and deployers of certain AI systems.[13]

The Colorado AI Act, effective February 1, 2026, requires both developers and deployers of high risk AI systems[14] to use reasonable care to avoid algorithmic discrimination in their AI systems. To create a rebuttable presumption of reasonable care, developers and deployers must take certain actions such as publishing information about their AI systems and instituting a human-review appeals process for adverse consequential decisions. While there is no private right of action associated with the Colorado AI Act, it is enforceable by the Colorado Attorney General and can carry penalties of up to $20,000 per violation. The Colorado AI Act applies so long as the developer or deployer does business in Colorado.

Federal AI Regulation

In contrast, 2024 did not bring significant new proposals for AI regulation at the federal level. One proposal in the House of Representatives in the last Congress, would require AI developers to disclose whether and which copyrighted works were used to train models.[15] The bill would need to be reproposed in the current Congress to move forward. Additionally, the National Institute of Standards and Technology has continued to provide non-binding guidance for managing AI risks.[16] And, as discussed further herein, some federal agencies

[13] The Colorado AI Act can be found here.

[14] Those that make, or are a substantial factor in making, a "consequential decision." Consequential decisions are those with a material legal or similarly significant effect on the provision or denial to any Colorado resident, or cost or terms of education, employment, financial/lending services, government services, healthcare, housing, insurance or legal services.

[15] The Generative AI Copyright Disclosure Act can be found here.

[16] See, for example the NIST Artificial Intelligence Risk Management Framework: Generative AI Profile that lays out 200+ suggested actions to mitigate the risk of generative AI, found here. Our previous discussion can found in our August 2024 blog post available here.

Compared to the U.S., the EU has been relatively proactive in regulating AI with its passage of the EU AI Act.

are using existing laws and regulations to promote responsible use and innovation of AI.

The EU AI Act

Compared to the U.S., the EU has been relatively proactive in regulating AI with its passage of the EU AI Act. The EU AI Act adopts a sliding scale of regulatory requirements depending on the level of risk posed by the AI system. Most AI systems currently used in the EU (*e.g.*, spam filters or AI-enabled video games) will likely be categorized as minimal risk and will not be covered by binding rules. The EU AI Act imposes stringent obligations with respect to AI systems classified as high risk[17] and outright prohibits a narrow set of AI system applications, including biometric categorization systems based on sensitive characteristics.

The EU AI Act also imposes specific obligations on providers of general purpose AI (GPAI) models, such as maintaining technical documentation of the model, providing detailed information to downstream providers, implementing a policy to comply with EU law on copyright and related rights and publishing a summary of the training data.[18] The EU AI Act further imposes specific transparency requirements on providers of certain consumer-facing AI systems (*e.g.*, chatbots), such as making users aware they are interacting with AI and labelling AI-generated content as such.

The EU AI Act has a broad jurisdictional hook, applying to any company whose AI is placed on the market or put into service in the EU, or whose AI output is used in the EU. The EU AI Act will apply directly across all EU member states, though most its provisions take effect only after a two-year transitional period. Failure to comply with its strictest provisions—those relating to prohibited AI systems—may result in fines of up to €35 million or 7% of group global annual turnover (whichever is higher). Non-compliance with most other provisions may result in fines of up to €15 million or 3% of group global annual turnover (whichever is higher).

AI Enforcement Actions in the U.S.

The SEC has recently ramped up its enforcement of AI washing claims. In March 2024, the SEC settled charges against two investment advisers, Delphia and Global Predictions, for false and misleading statements about their AI capabilities in violation of the Advisors Act.[19] According to the SEC, Delphia falsely claimed to use machine learning in its investment selections, and Global Predictions falsely claimed to be the "first regulated AI financial adviser" and exaggerated its use of "expert AI-driven forecasts." Similarly, in June 2024, the SEC charged the CEO and founder of AI recruitment startup Joonko for misrepresenting the sophistication of its automation technology. The SEC emphasized that investors "considered the state of Joonko's technology important in deciding whether to invest."[20] While AI washing made up only a small piece of SEC enforcement in 2024, emerging financial technologies, including AI, are currently a component of the SEC's examination priorities for 2025.[21] For further discussion, *see* An Active Year in Enforcement, with Changes to Come.

[17] AI systems are considered high-risk if they pose a "significant risk" to an individual's health, safety, or fundamental rights, and, in particular, if: (i) they are intended to be used as a product or as a safety component of a product covered by EU harmonization legislation listed in Annex I (*e.g.*, medical devices, industrial machinery, toys, aircraft, and cars) and the product is required to undergo a third-party conformity assessment under the above-mentioned legislation; or (ii) they are used in certain contexts listed in Annex III (*e.g.*, AI systems used for education, employment, critical infrastructure, essential services, law enforcement, border control, and administration of justice). Obligations relate to risk management system, data governance, technical documentation, transparency, registration and record-keeping requirements and human oversight, as well as accuracy, robustness and cybersecurity.

[18] A GPAI model is defined as an: "*AI model* [...] *that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications*".

[19] For further information, please see the SEC's March 2024 press release here.

[20] For further information, please see the SEC's June 2024 press release here.

[21] The SEC's 2025 Examination Priorities can be found here.

Meanwhile, the FTC, in an enforcement sweep dubbed "Operation AI Comply" took action under the FTC Act against multiple companies using AI to engage in allegedly deceptive or unfair trade practices, such as promoting an AI tool used to create fake product reviews, providing an "AI Lawyer" service and selling products that claimed to use income-generating AI. The FTC is focused on combating AI systems "designed to deceive" and bogus claims of AI capabilities made to deceive consumers.

AI Governance Considerations

Over the next 24 months, more companies are expected to implement advanced, tailored AI solutions, in the hope of still greater benefits.[22] These opportunities to build a more competitive business should be a discussion topic for every board of directors and senior management team, and so too should the framework for evaluating and overseeing the attendant risks.

Risk Assessment Framework

For efficient yet measured governance, companies should consider implementing a risk assessment framework of delegation to vet low-risk AI tools and escalation to vet high-risk AI tools.

Risk "scorecards" can be used to internally standardize an initial risk assessment of proposed AI tools. Under this approach, the risk assessment team assigns a score to each category of risk (commercial risk, legal and regulatory risk, reputational risk, *etc.*) based on the likelihood of a liability-creating or otherwise damaging event and the potential impact of the event. Preparation of sample scorecards (*i.e.*, for AI tools already vetted and deployed) may be a useful exercise for gaining perspective on the overall levels of risk represented by these scores.

This system of escalation affords boards and senior management the opportunity to make strategic decisions with respect to high-risk, high-reward AI use-cases while streamlining adoption of well-tested, low-risk AI tools. Outlined below are a few key considerations for boards when designing AI governance protocols.

[22] *See* Microsoft, "IDC's 2024 AI opportunity study: Top five AI trends to watch" (November 12, 2024), available here.

Regardless of which strategy they adopt, boards and senior management should consider the benefits of creating a dedicated internal AI team or taskforce to assess the selection, implementation and risks of the chosen strategy.

AI Strategy: Risk Implications of Build versus Buy

The decision to build or buy generative AI solutions is primarily a commercial decision, but with meaningful risk implications. Only a small percentage of companies are building generative AI solutions fully in-house. Those that do may incur significant expense,[23] but they exercise more control over the technology, have the ability to customize it to their specific needs and can mitigate risks associated with outsourced AI infrastructure, such as data privacy.[24] Most companies have instead opted to buy or lease generative AI from third-party vendors or have partnered with vendors to build generative AI solutions, which can reduce development expense but increases third party risk exposure.[25]

Regardless of which strategy they adopt, boards and senior management should consider the benefits of creating a dedicated internal AI team or taskforce to assess the selection, implementation and risks of the

[23] *See* Time, "The Billion-Dollar Price Tag of Building AI" (June 3, 2024), available here.

[24] *See*, *e.g.*, EY, "How organisations can choose between buying and building AI systems" (February 19, 2024), available here.

[25] KPMG surveyed 225 senior business leaders at companies with revenue greater than or equal to $1 billion in August 2024. Only 12% of companies are building generative AI in-house. 50% are buying or leasing generative AI from vendors, and 29% are pursuing a mix of building, buying, and partnering. *See* KPMG, "GenAI Dramatically Shifting How Leaders Are Charting the Course for Their Organizations" (August 15, 2024), available here.

chosen strategy. Responsibilities of such a team would include conducting due diligence on external AI tools,[26] fine-tuning AI models with company-specific data[27] and auditing existing AI models.[28] In particular, as more AI models are trained using synthetic (*i.e.*, AI-generated) training data,[29] boards and management teams should be aware of the associated risks and appropriate safeguards.[30]

AI-Related Cybersecurity Risks

The FBI has warned about an increasing threat of cyber criminals using AI in cyberattacks, such as AI-driven phishing and AI-powered voice and image fraud.[31] Cyber criminals also target AI models themselves. Sophisticated cyberattacks on AI models, including data reconstruction attacks, create significant risk when the model is trained on highly sensitive data.[32] Some examples of highly sensitive data are health data, consumer data and personally identifiable information.[33]

Management teams, under board supervision, should have a protocol for scrutinizing the cybersecurity and debugging safeguards of every AI tool used in their companies, with input from internal cybersecurity, information technology and AI teams. With external AI tools, such as enterprise or open source AI, management should consider the single point of failure risk that, in the worst case, can lead to industry-wide crisis like the CrowdStrike outage.[34]

Accounting for AI Error

Because generative AI models are designed to be creative, some experts believe AI hallucination is not a solvable problem.[35] Yet, as the technology improves, there is a risk that employees might become over-reliant on AI and too trusting of its results.[36] There is also the potential black-box problem, where AI users are unable to understand how the AI makes decisions due to its complexity.[37]

Employees must be adequately trained to integrate AI into their work while also monitoring AI output for errors. In addition, boards of companies that manage sensitive or confidential data should ensure employees are aware of risks in submitting that data to AI products sold or leased by third parties.

[26] For a risk assessment guide for AI vendors, *see* FS-ISAC, "Generative AI Vendor Risk Assessment Guide" (February 2024), available here, For a risk assessment guide for open source AI tools, *see* LeadDev, "Be careful with 'open source' AI" (August 20, 2024), available here.

[27] *See*, *e.g.*, IBM, "What is fine-tuning?" (March 15, 2024), available here.

[28] For a general explanation of AI auditing, *see* Salesforce, "Are you ready for an AI audit?" (June 17, 2024), available here.

[29] *See*, *e.g.*, IBM, "Examining synthetic data: The promise, risks and realities" (August 20, 2024), available here.

[30] Recent research has shown that indiscriminate use of online AI-generated text to train large-language models may cause irreversible defects in the resulting AI model, also known as model collapse. Shumailov et al., "AI models collapse when trained on recursively generated data" (July 24, 2024), available here.

[31] FBI, "FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence" (May 8, 2024), available here.

[32] For a more comprehensive overview of cybersecurity attacks on AI models, *see* Zohra El Mestari et al., "Preserving data privacy in machine learning systems" (February 2024), available here.

[33] Health information is protected by the HIPAA Privacy Rule. *See* U.S. Department of Health and Human Services, "The HIPAA Privacy Rule," available here. Consumer privacy laws have been passed in 20 states. Bloomberg Law, "Twenty States Have Consumer Privacy Laws; More Likely to Come" (September 13, 2024), available here. For an overview of personally identifiable information, *see*, *e.g.,* National Institute of Standards and Technology, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)" (April 2010), available here.

[34] For a discussion on single point of failure risks generally, *see* Law. com, "CrowdStrike Glitch Highlights Risk of Single Point of Failure in Cybersecurity" (July 30, 2024), available here. For a discussion on the concentration of generative AI technologies, *see* MIT Technology Review, "Make no mistake—AI is owned by Big Tech" (December 5, 2023), available here.

[35] *See* Scientific American, "AI Chatbots Will Never Stop Hallucinating" (April 5, 2024), available here.

[36] *See* Stanford University, "Artificial Intelligence Index Report 2024," Chapter 4, page 64 (May 2024), available here.

[37] For a discussion on AI's black box problem, *see* World Economic Forum, "Building trust in AI means moving beyond black-box algorithms. Here's why" (April 2, 2024), available here.

Key Takeaways

- Novel AI copyright issues are being litigated, and courts will soon provide at least some answers to questions, such as the application of the fair use doctrine to various uses of AI.

- Though federal AI legislation is not expected soon, state lawmakers have been relatively proactive with respect to AI, addressing issues such as employment and consumer protection. Likewise, the EU has adopted its own comprehensive AI regulatory scheme with broad jurisdiction.

- Even without new AI-specific legislation, federal agencies have shown willingness to engage with AI-related issues and bring enforcement actions under existing law.

- With the variety of legal risks in mind, a risk assessment framework designed around a combination of delegation and escalation lets boards and management streamline the AI vetting process and appropriately shifts board-level focus to high-risk AI tools.

- Boards should consider the specific benefits and drawbacks of relying on third-party vendors versus in-house generative AI creation; each option offers different benefits and presents a different risk profile.

- It remains critical for companies to prioritize updating their cybersecurity infrastructure and risk frameworks for the rollout of generative AI.

- Corporate adoption of AI tools presents unique employee-level risks, the mitigation of which will require more than just vetting.

Focus on SEC Executive Compensation Disclosure Obligations in 2025: Security Costs and New Item 402(x)

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

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

Ariel Adler
Associate
New York
aradler@cgsh.com

Wil Armand Steebs
Law Clerk
New York
wsteebs@cgsh.com

Heading into 2025, boards of directors must be prepared to address both rising concerns around executive security costs and new Securities and Exchange Commission (SEC) disclosure rules relating to the timing of option and stock appreciation right (SAR) awards. We discuss the issues directors should consider below.

Executive Security During Volatile Times

The recent killing of UnitedHealthcare Group's insurance division CEO Brian Thompson outside a New York City hotel while he was attending the company's annual investor meeting has brought executive security into sharp focus for many boards of directors heading into 2025.[1] Although companies may conclude that providing personal security benefits outside of business engagement to CEOs or other senior executives is necessary to protect the company's human capital assets, the SEC has to date been clear that these expenses should be disclosed as perquisites to the impacted executives[2] and we thus far have not seen any indication that the SEC's views will shift during the current proxy season. That said, investor perspectives with respect to security-related expenses may well shift as a result of the very serious and tangible risks to key management. Below, we discuss key issues associated with

[1] *See* Chip Cutter, Theo Francis & Andrew Tangel, "UnitedHealth Shooting Is a Wake-Up Call on Corporate Security" (December 5, 2024), available here.

[2] One recent example is the SEC's recent settlement with the Greenbrier Companies Inc. and certain of its executives for failing to disclose certain perquisites, including personal security costs. *See* Securities and Exchange Commission Press Release, "SEC Charges Global Transportation Company Greenbrier and Former CEO for Failing to Disclose Perks and Payments" (March 2, 2023), available here.

Investor perspectives with respect to security-related expenses may well shift as a result of the very serious and tangible risks to key management.

executive security costs and the related disclosure that directors should take into account.

- **Companies Disclosing Security Expenses**: According to data from Equilar cited by the *Wall Street Journal*, just over a quarter of S&P 500 companies disclosed providing personal security services as a perquisite to CEOs in 2023, while only about 13% disclosed providing personal security services to executives other than the CEO.[3] Given recent events, absent a change in the SEC's position on personal security protection we would expect these numbers to rise significantly, especially among companies that have identified specific threats, conduct business in controversial fields or engage with consumers and other stakeholders in emotionally charged settings. We also anticipate companies may increase security protection provided to executives while engaged in business and on business-related travel and otherwise engaged in business-related activities, which (under current SEC guidance) would not be disclosed as a perquisite.

- **Disclosure Obligations**: Security arrangements for named executive officers (NEOs) often need to be disclosed in a company's annual proxy statement as a perquisite, depending on the nature of the expense. According to the SEC, an item is not considered a perquisite or personal benefit if it is "integrally and directly related" to the performance of the executive's duties.[4] The SEC has stated that the concept of a benefit that is "integrally and directly related" to job performance is a narrow one.[5] Whether the company has determined that an expense is an "ordinary" or "necessary" business expense for tax or other purposes, or whether it is for the benefit or convenience of the company, is not relevant when determining if the expense should be considered a perquisite for disclosure purposes.[6] Security costs that qualify as NEO perquisites need to be disclosed and identified in the company's annual proxy statement if the NEO receives over $10,000 in total perquisites.[7] When disclosing these costs as perquisites, many companies try to mitigate the impact of the disclosure (including criticisms by proxy advisory firms, such as ISS, about the magnitude of personal security costs) by noting that they consider the security expenses for personal travel and/or family to be appropriate business expenses that arise from the executive's employment responsibilities, necessary to his or her job performance and aimed at ensuring the safety of the covered executive and his or her family. We anticipate that recent events will result in issuers doubling down on these sorts of disclosures to justify what will likely be increased expenditures on security costs that, despite the business justifications, are likely to require perquisite disclosure under the current SEC rules. Below, we discuss key examples of security costs that may be disclosed as personal expenses and others that the SEC may consider business expenses:

  - ***Business Trips***: If a company provides security for an NEO's business meetings or attendance at a company business event, such as an annual investor meeting, these costs would be considered "integrally and directly related to the performance of the executive's duties" and, therefore, would not require disclosure.

  - ***Personal Vacations***: Many companies have policies that, for security purposes, require certain

[3] *See* Cutter et al. *supra* note 1.

[4] *See* Securities and Exchange Commission "Executive Compensation and Related Person Disclosure, Release No. 33-8732A" (August 29, 2006) at 74, available here (the SEC Release).

[5] *Id.* at 75.

[6] *Id.* In many instances, an issuer's board of directors may commission a "security study" in an effort to document a bona-fide security threat and to support, for federal income tax purposes, the deductibility of personal security related costs. To date, the SEC has not indicated that studies supporting enhanced security measures for a company's named executive officers would justify a conclusion that personal security costs are not perquisites.

[7] 17 CFR § 229.402(c)(ix)(A).

executives (or their families) to use company aircraft for personal travel or company-provided property for vacations. If an NEO is traveling with family on a personal vacation and the company provides security for the trip or mandates the use of company-provided property or aircraft, the security costs (as well as the use of the aircraft or property) should be disclosed as a perquisite, even if the company deems the security a necessary business expense.

- ***Family Attending Business Events***: If an NEO's family members attend a business-related event, the incremental costs associated with security for the NEO's family members should be disclosed as a perquisite.[8]

- ***Company-Sponsored Entertainment Events***: If an NEO is traveling to an entertainment event where the company has a sponsorship relationship, such as a sporting event, the security provided for the trip may need to be disclosed as a perquisite, even if there is a business purpose due to the company's sponsorship of the event. This is a grey area, and the facts and circumstances will be critical to the analysis. For example, if the NEO's attendance is mandated by the terms of a sponsorship agreement (*e.g.*, to present an award or fulfill other duties on behalf of the company) then there may be grounds to determine that the security provided is not a perquisite. However, given the spotlight on these issues from the SEC and the fact that shareholders and proxy advisory firms may be more accepting of security costs and related disclosure in the wake of recent events, a more conservative approach is often advisable in these types of situations.

- ***Commuting***: Security provided for commuting to and from work, including a company-provided car and driver is considered a perquisite that requires disclosure since commuting costs are a per se perquisite under the SEC rules.[9]

- **How Security Costs Are Calculated for Disclosure Purposes**: For proxy disclosure purposes, companies typically only disclose the approximate aggregate incremental cost for non-business-related security. In order to calculate these costs correctly, boards of directors and compensation committees need to ensure that management has established effective controls and procedures for identifying and valuing perquisites (including, for example, proper tracking processes, training programs and guidelines for how to handle specific perquisite issues), since gathering the relevant information in real time is critical to ensuring accurate year end disclosure when preparing a proxy statement. It is also important to note that the calculations for security costs in proxy disclosures often differ from those used for accounting or tax reporting purposes. Therefore, companies should consult with tax and legal advisors when considering security policies and as new fact patterns emerge to ensure that executive security costs are not only appropriately monitored and tracked over the course of the year in a manner that is appropriate for all relevant purposes, but also calculated correctly for each such purpose.

A Year in Review: New Item 402(x)

On December 14, 2022, the SEC adopted new disclosure requirements under Item 402(x) Regulation S-K requiring disclosure of a company's policies and practices on the timing of option and 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). For calendar year-end companies, the upcoming proxy statement reporting on fiscal year 2024 equity grants will be the first time Item 402(x) disclosure is required. Below, we briefly highlight the requirements of Item 402(x) and share impressions from its first full fiscal year in effect.

[8] In certain instances where the incremental costs are de minimis or not calculable on a per person basis, issuers often include general narrative footnote disclosure in the Summary Compensation Table (SCT) describing the perquisite, but not attributing any monetary value in the "All Other Compensation" column of the SCT.

[9] SEC Release at 77.

Recap

- **Narrative Disclosure**: Item 402(x) requires 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 material nonpublic information (MNPI). Companies are required to include this narrative disclosure regarding their policies and practices regardless of whether the company has actually made grants of options, SARs or option-like awards close in time to the release of MNPI. It is worth noting that Item 402(x) also requires disclosure as to "whether the registrant has timed the disclosure of material nonpublic information for the purpose of affecting the value of executive compensation."[10] Many issuers have interpreted this aspect of the rule to require disclosure in respect of their equity grant timing practices with regard to all types equity incentive awards (including restricted stock units and performance stock units). This has typically resulted in simple disclosures stating that the issuer does not schedule equity award grants in anticipation of the release of MNPI, nor does it time the release of MNPI based on equity grant dates.

- **Tabular Disclosure**: If a company has awarded options or SARs to a NEO within the period starting four business days before and ending one business day after the filing or furnishing of a periodic or current report (excluding an 8-K disclosing the new option award, but including an earnings release) that discloses MNPI, Item 402(x) requires tabular disclosure of the following: (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.

A growing number of issuers, however, are considering shifting their option grant practices to intentionally avoid tabular disclosure in future years, frequently by stipulating the grant date of any option or SAR to be two or more business days following the filing date of any MNPI.

Year in Review

While all issuers must include narrative disclosure required by Item 402(x), tabular disclosure is only required of those issuers that grant options or SARs within the window designated by the rule. This tabular disclosure largely synthesizes information already publicly available, and as a result we have seen many issuers remain comfortable with their existing option grant process even if they trigger inclusion of the Item 402(x) table. A growing number of issuers, however, are considering shifting their option grant practices to intentionally avoid tabular disclosure in future years, frequently by stipulating the grant date of any option or SAR to be two or more business days following the filing date of any MNPI. As a result, it is advisable for boards and compensation committees to review their existing equity grant policies and practices and consider whether any changes are appropriate in light of these disclosure requirements, as well as other recent SEC guidance such as Staff Accounting Bulletin 120, which provides guidance about proper recognition and disclosure of compensation cost for "spring-loaded" awards made to executives of the issuer.

[10] Item 402(x)(1) of Regulation S-K.

Non-Competes: One Step Forward and Two Steps Back

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

Eitan Agagi
Associate
New York
eagagi@cgsh.com

Emily C. Barry
Associate
New York
ebarry@cgsh.com

Maisha Kamal
Associate
New York
mkamal@cgsh.com

In 2024, two federal agencies saw challenges to their regulations restricting non-compete agreements, while several states enhanced restrictions or proposed amendments expanding existing non-compete laws. The scope and impact of these developments are likely to be further clarified as legislation and new case law develops.

FTC Rule

In early 2024, the Federal Trade Commission (FTC) issued a final rule banning most existing and new non-competes, broadly including any covenant or mix of covenants that "function to prevent a worker from joining a competitor."[1] The rule covered all U.S. employees, including senior executives, with exceptions for (i) non-competes entered into in connection with the bona fide sale of a business; (ii) existing non-competes with senior executives, defined as workers in a "policy-making position" who earn more than $151,164 annually; and (iii) contracts between a franchisee and a franchisor. The rule also required that employers provide notice to workers who are subject to a non-compete provision that the non-compete will not and cannot legally be enforced against them.

[1] FTC, "FTC Announces Rule Banning Noncompetes" (April 23, 2024), available here.

Although the rule's scheduled effective date was September 4, 2024, it faced many legal challenges and, on August 20, 2024, was vacated by a federal court in Texas on a nationwide basis. The FTC challenged that decision in a notice of appeal on October 18, 2024[2] and the FTC also defended the rule in an Eleventh Circuit appeal on November 4, 2024.[3] Further challenges are likely to be seen in 2025, and we anticipate it will be some time until final decisions are rendered by the courts. For now, the rule remains vacated and state law currently controls the applicability of any non-compete and other restrictive covenants.

NLRB Enforcement

The National Labor Relations Board's (NLRB's) May 2023 memorandum stating that most non-compete agreements violate the National Labor Relations Act has spurred a number of enforcement actions, one of which has altered the framework the NLRB utilizes to assess the validity of restrictive covenants. In August 2023, the NLRB decided to adopt a new burden-shifting framework for restrictive covenants that requires evaluating whether a facially neutral work rule or policy could reasonably be interpreted to be coercive "from the perspective of an employee who is subject to the [challenged] rule and economically dependent on the employer."[4] If that burden is met, the NLRB will find the rule presumptively unlawful, though the presumption can be rebutted by the employer with adequate evidence.

The framework has been used in subsequent cases, one of which involved rescinding non-compete provisions in an employment agreement on the grounds that they chilled union-organizing activity.[5] In the case, an employee who engaged in "salting," a practice that involves taking a non-union job intending to organize a workforce, was discharged by their employer.

[2] *See Ryan, LLC v. Federal Trade Commission* (N.D. Tex. August 20, 2024).

[3] *See Properties of the Villages Inc. v. Federal Trade Commission* (M.D. Fla. August 15, 2024).

[4] NLRB Office of Public Affairs, "Board Adopts New Standard for Assessing Lawfulness of Work Rules" (August 2, 2023), available here.

[5] *See J.O. Mory, Inc. and Indiana State Pipe Trades Ass'n a/w United Assn. of Journeymen and Apprentices of the Plumbing and Pipefitting Indus. Of the United States and Can., AFL-CIO* (June 13, 2024).

The challenged non-compete provisions prohibited employees from soliciting or persuading other employees of the employer to leave their employment and engaging or working in any other similar or competitive businesses following their separation from the employer. The provisions also required the employee to report any solicitation offers they received. In June of 2024, the NLRB found these provisions to be in violation of the National Labor Relations Act and ordered their recission.

State Developments

Restrictions on non-compete clauses have also been developing rapidly at the state level. Currently, total bans on non-competes are in effect in California (whose retroactive notice requirement went into effect on January 1, 2024, with a deadline for compliance shortly thereafter), North Dakota, Oklahoma and, most recently, Minnesota. Building on its existing non-compete ban, the Minnesota House proposed a bill, HF 3456, that would apply to service providers and prohibit restrictive covenants in service contracts, intending to close a loophole in its current non-compete ban that allows service providers to subject employees to non-solicit and no-hire restrictions through intercompany contracts. This bill was scheduled for further action in the Minnesota House on March 7, 2024, but thus far no further action has been taken.

In Delaware, a January 2024 ruling by the Delaware Supreme Court reversed a previous decision by the Court of Chancery and upheld the enforceability of restrictive covenants in partnership agreements, which conditioned distributions on partners' compliance with non-compete and non-solicit provisions.[6] As the subsequent application of this case has created some ambiguity for courts reviewing provisions governed by Delaware law, the Seventh Circuit recently certified two questions to the Delaware Supreme Court about the scope of the ruling, for which arguments were heard on October 9, 2024.

[6] *See Cantor Fitzgerald, L.P. v. Ainslie,* C.A. No. 9436 (Del. January 29, 2024).

Employers should catalog where employees are located and be prepared to track both current and former employee mobility to ensure compliance with non-compete restrictions.

In Massachusetts, *Miele v. Foundation Medicine Inc.*, a case decided this past July, clarified that the Massachusetts Noncompetition Act (MNAA) does not apply retroactively from its effective date of October 1, 2018, though the court held that reaffirmation of an existing agreement creates a new agreement for purposes of the effective date. The court also held that forfeiture-for-competition provisions, which are covered under the MNAA, include non-solicits and no-recruit covenants. On November 4, 2024, the defendant filed its opening brief in an application for direct appellate review.

Finally, Washington amended its non-compete laws with Senate Bill 5935 (S.B. 5935), effective June 6, 2024, which expanded the definition of "non-competition covenant" to include agreements that directly or indirectly prohibit the acceptance or transaction of business with a customer. Employers should be focused on a few key aspects of the amendments, namely that employers must disclose non-competition covenants to prospective employees by the time of an employee's initial acceptance of an employment offer, regardless of whether the offer is oral or written. Additionally, the amendment clarified that a person aggrieved by a noncompetition covenant, regardless of whether or not they were a party to the covenant, can pursue relief.

Next Steps

As an ongoing matter, employers should catalog where employees are located and be prepared to track both current and former employee mobility to ensure compliance with non-compete restrictions, review and revise form agreements for any potentially void non-compete clauses and continue to consult with counsel and monitor these and other developments over the coming year.

An Active Year in Enforcement, with Changes to Come

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

Lisa Vicens
Partner
New York
evicens@cgsh.com

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

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

Ava Bayani Kazerouni
Associate
Washington, D.C.
akazerouni@cgsh.com

The Securities and Exchange Commission (SEC) and Department of Justice (DOJ) both had active enforcement years in 2024. The SEC's aggressive focus on crypto enforcement continued, resulting in the filing and continued litigation of several cases in federal courts nationwide. The DOJ announced a number of policy updates in 2024, including guidance related to voluntary disclosures and corporate enforcement, and remained active in the foreign corruption and national security spaces. Finally, both the SEC and DOJ have increased their focus on AI and new technologies, showing increasing concern about the risks associated with AI, with the DOJ issuing guidance on AI in compliance programs and the SEC bringing cases related to misleading marketing about the use of AI in investment strategies. As noted more fully below, with the incoming Trump Administration, enforcement priorities at both SEC and DOJ are expected to shift. The SEC is expected to have a renewed focus on traditional enforcement areas, such as accounting fraud, misrepresentations in securities offerings and insider trading, with significant reductions in enforcement activity related to crypto, cyber incidents and ESG issues. The DOJ is likely to continue its focus on FCPA and national security (including sanctions and export controls), while devoting increasing resources to

immigration and violent crime. Additionally, the benefits of cooperation are likely to increase at both the SEC and DOJ, with the potential for reduced penalties for companies able to effectively demonstrate their cooperation and self-remediation.

In anticipation of the incoming Trump Administration, there already have been notable personnel changes at both SEC and DOJ with more to come. Specifically, SEC Chair Gary Gensler and Democratic Commissioner Jaime Lizarraga have announced that they will depart. In addition, Trump has announced the nomination of former Commissioner Paul Atkins as Chair, who will stand to replace the outgoing heads of the Divisions of Enforcement and Corporation Finance, among other positions. On the DOJ side, Attorney General-nominee Pam Bondi and Deputy Attorney General nominee Todd Blanche will work with all-new appointees at the top levels of DOJ. Most of the nominees for those positions have yet to be announced, though the incoming administration has announced the nomination of Gail Slater to head the Antitrust Division and Kash Patel to run the FBI.

Key SEC Developments

The SEC filed 583 total enforcement actions in 2024, a 26% decline from the previous year.[1] Total financial remedies reached $8.2 billion, the highest amount in SEC history and a large increase from the $4.9 billion received in 2023, though more than half that total was attributable to a judgment obtained after the SEC's jury trial win against blockchain startup Terraform Labs and its founder, Do Kwon.[2] The SEC also continued setting records with its whistleblower program, receiving more than 24,000 whistleblower tips and announcing whistleblower awards of more than $255 million.[3] In announcing their year-end results, the SEC highlighted the importance of self-reporting, noting that "market participants across the spectrum—from public companies to major broker-dealers and advisory firms—stepped up efforts to self-report, remediate, and meaningfully cooperate with our investigations."[4] The SEC also extolled the virtues of cooperation and remediation by entities facing enforcement investigations, with benefits including reduced or no penalties. The benefits of cooperation are likely to increase under the new administration. Substantively, the SEC maintained its focus on digital assets and traditional areas such as accounting, financial disclosure, and oversight of investment advisers and other regulated entities.

The benefits of cooperation are likely to increase at both the SEC and DOJ, with the potential for reduced penalties for companies able to effectively demonstrate their cooperation and self-remediation.

Artificial Intelligence

The SEC's ramp-up of AI oversight included enforcement actions, new examination priorities, and proposed rulemaking. For example, in March 2024, the SEC announced two enforcement actions against investment advisers for "AI-washing" and violations of the Marketing Rule, alleging that the relevant investment advisers had marketed that they were using AI in certain ways that they allegedly were not. For further discussion, *see* Effective Board Oversight as AI Evolves.

Digital Assets

Digital assets remained at the forefront of the SEC enforcement agenda, with the agency continuing to bring litigated cases rather than to pursue rulemaking. The SEC continued high-profile litigation cases against

1 SEC Press Release, "SEC Announces Enforcement Results for Fiscal Year 2024," (November 22, 2024), available here (SEC Year in Review).

2 *Id.*; SEC Press Release, "Terraform and Kwon to Pay $4.5 Billion Following Fraud Verdict," (July 2, 2024), available here.

3 SEC Year in Review, *supra* note 1.

4 *Id.*

We expect the SEC under the new administration likely will conduct fewer sweeps designed to condition the behavior of the securities industry.

three digital asset trading platforms, which are set to extend into 2025.[5] The cases were brought in three different jurisdictions, with the courts so far agreeing only that the digital assets themselves are not securities and that the manner in which the digital asset is sold determines whether there is a securities transaction.[6] After focusing on digital asset issuers and platforms, the SEC for the first time targeted a market maker in connection with its role in facilitating the trading of digital assets. The industry will be paying close attention to these cases that target digital asset infrastructure in the next year. With the nomination of Paul Atkins as Chair, the SEC may take a more restrained approach to digital asset enforcement by turning back to potential rulemaking, if enabled by Congress, instead of litigation, to address this new technology. As such, the SEC is expected to bring fewer cases in this space, likely only where there is potential fraud in the offering of a digital asset. With respect to ongoing litigation, where there is no allegation of fraud or investor harm, the SEC is likely to look for easy settlements or will potentially dismiss cases.

Off-Channel Communications

The SEC continued its sweep of regulated entities' use of "off-channel communications," assessing over $600 million in penalties in settled actions against over 70 broker-dealers, investment advisors, municipal advisors and credit-rating agencies that allegedly did not comply with recordkeeping requirements in connection with employees' use of texting or messaging apps.[7] This initiative has likely run its course, as the two Republican Commissioners who will remain on the SEC have called on the agency to "reconsider [the] current approach to the off-channel communications issue."[8] More generally, we expect the SEC under the new administration likely will conduct fewer sweeps designed to condition the behavior of the securities industry and instead focus more of its resources on cases that involve actual investor harm, such as offering frauds, accounting and issuer disclosure fraud and misappropriation of funds by investment advisers.

Cybersecurity

Cybersecurity has risen to the top of the SEC's list of enforcement priorities. In late 2023, the SEC's new rules on cyber disclosures took effect, which, among other things, require disclosure on Item 1.05 of Form 8-K within four business days after a registrant determines that it has experienced a material cybersecurity incident.[9]

While the SEC has continued to bring settled cases in this space, it was dealt a significant setback when a court dismissed most SEC fraud claims related to allegedly misleading statements by the software company SolarWinds and its chief information security officer in connection with a massive, state-sponsored cyber intrusion the company suffered.[10] A judge in the Southern District of New York held that most of the company's statements about its cybersecurity defenses were too generalized to be materially misleading and that the internal controls provisions of the securities laws were meant to apply to accounting controls rather

[5] SEC Press Release, "SEC Files 13 Charges Against Binance Entities and Founder Changpeng Zhao," (June 5, 2023), available here; SEC Press release, "SEC Charges Coinbase for Operating as an Unregistered Securities Exchange, Broker, and Clearing Agency," (June 6, 2023), available here; SEC Press Release, "SEC Charges Kraken for Operating as an Unregistered Securities Exchange, Broker, Dealer, and Clearing Agency," (November 21, 2023), available here.

[6] This approach was first devised by the court in 2023 in an SEC litigation against crypto and blockchain technology company, Ripple Labs Inc., its CEO Brad Garlinghouse and its former CEO and Executive Chairman Christian Larsen. For more information on Cleary Gottlieb's representation of Ripple Labs Inc. CEO Brad Garlinghouse, *see* our October 2023 blog post available here.

[7] SEC Year in Review, *supra* note 1.

[8] SEC Statement, "A Catalyst: Statement on Qatalyst Partners LP," (September 24, 2024), available here.

[9] SEC Statement, "Cybersecurity Disclosure," (December 14, 2023), available here.

[10] For more information on the SDNY Court's Dismissal of SEC Claims Against SolarWinds and CISO, *see* our July blog post available here.

than cybersecurity controls. The court did, however, allow the SEC to proceed on claims that SolarWinds allegedly misled investors by posting a "security statement" on its website that touted its adherence to specific cybersecurity standards that, in the SEC's view, it was not following. The SolarWinds case, which led to a sweep-style investigation of companies impacted by the breach, symbolized the priority the SEC attached to detailed disclosures of the potential impact of cyber incidents, as demonstrated by multiple enforcement actions in the last several years against companies that were themselves the victims of cyber attacks. In the wake of the court ruling, as well as statements by the Republican commissioners who objected to bringing the SolarWinds case and similar cases targeting victims of cyber-attacks, the SEC is likely to temper its backward-looking scrutiny of companies' post-incident disclosures and refrain from charging internal controls violations in cybersecurity cases where the company's accounting and disclosure controls are not specifically implicated.[11]

Key DOJ Developments

In 2024, the DOJ published a number of policy updates and guidance in areas related to corporate enforcement, compliance and the use of AI. This focus was similarly reflected in the hiring of personnel, such as the department's first Chief Science and Technology Advisor and Chief Artificial Intelligence Officer.[12] Through these policies, the DOJ continued its strategy of incentivizing voluntary self-disclosure by providing specific and quantifiable benefits for self-reporting, including by rolling out a new whistleblower awards pilot program offering bounty payments to individual whistleblowers. The incoming Trump Administration will want to make their imprint through their own DOJ policies, as such we may expect them to withdraw or revise policies that raise the bar on what is required for companies to receive leniency, while keeping in place policies that benefit corporate defendants.[13] In 2024, the DOJ remained focused on corporate enforcement in areas such as FCPA, anti-money laundering, digital assets, and, increasingly, on national security, which is likely to continue with the incoming Trump Administration.

Policy Updates and Guidance

The DOJ issued a number of important policy updates and guidance throughout 2024, with a continued focus on voluntary self-disclosure and ratcheting up pressure on companies to be "first in the door" to self-report misconduct. The DOJ policies seek to achieve this objective by rewarding whistleblowers with monetary awards; offering non-prosecution agreements to culpable individuals who provide actionable information; providing safe harbor for acquiring companies who self-report criminal conduct by an acquired company; and a continued emphasis on maintaining an effective compliance program. These policies are:

- **Mergers & Acquisitions Safe Harbor**: In another iteration of its emphasis on self-reporting, the DOJ revised the Justice Manual to include a "safe harbor" from prosecution for acquiring companies that self-report criminal conduct by an acquired company identified in due diligence. The Safe Harbor, implemented in March 2024, provides a presumption in favor of DOJ declining to prosecute an acquiring company that voluntarily and promptly self-reports criminal violations by an acquired company, remediates any misconduct and forfeits proceeds of the violation.[14] However, additional requirements apply to potential criminal Sherman Act violations. The Safe Harbor provision does not permit compliant companies that report criminal violations of the Sherman Act by a target to close their acquisition until

[11] The Republican commissioners also dissented from four cases brought in the Fall, which claimed that IT companies victimized by the SolarWinds cyber intrusion had misleadingly downplayed the incident in their disclosures.

[12] DOJ Press Release, "Attorney General Merrick B. Garland Designates Jonathan Mayer to Serve as the Justice Department's First Chief Science and Technology Advisor and Chief AI Officer," (February 22, 2024), available here.

[13] This was the case in the prior Trump Administration, where, for example, they withdrew the Yates Memo, which focused on individual accountability for corporate misconduct, as well as revised the guidance on monitorships to clarify that the DOJ would appoint a monitor in connection with a resolution only in limited circumstances where there was a "demonstrable need."

[14] Justice Manual §§ 9-28.900(A)(3)(a)(i), 9-28.900(B); §§ 703.300, 9.28.900(A)(3)(c) (March 2024).

the DOJ Antitrust Division provides a conditional leniency letter or allows the leniency marker to expire, making it an impractical option for the majority of purchasers.[15]

- **The Pilot Program on Voluntary Self-Disclosure for Individuals**: In April, the DOJ launched a Pilot Program on Voluntary Self-Disclosure for Individuals to incentivize culpable individuals to self-report their misconduct and cooperate in the DOJ's investigation and prosecution of other individuals and companies in exchange for non-prosecution agreements (NPAs).[16] Culpable individuals can qualify for an NPA if they are first to report and provide substantial assistance to the prosecution of more culpable individuals or companies in certain core enforcement areas.[17]

  The DOJ programs effectively create a race between companies and individuals to report misconduct, as an individual must be "first in the door" in order to receive an NPA or whistleblower award.[18] This likely will leave companies at a disadvantage as it is often easier for individuals to have an understanding of their role in misconduct as compared to companies, especially large, multinational companies. As culpable individuals may be incentivized to report directly to DOJ, companies will need to balance conducting thorough, confidential and complete internal investigations with maintaining confidentiality so as not to "tip off" individuals involved in the misconduct. As the whistleblower and individual self-disclosure programs are pilot programs, it is possible the Trump Administration will not renew them.

- **Whistleblower Awards Pilot Program**: The DOJ's Whistleblower Awards Pilot Program, launched last August, provides individuals with awards of up to $50 million if they provide original information and cooperate in an investigation leading to more than $1 million in criminal or civil forfeiture in connection with a successful DOJ case related to corporate criminal conduct.[19] Notably, companies that receive internal whistleblower reports are still eligible to obtain credit and the presumption of a declination even if the whistleblower also reported to DOJ, so long as the company (1) self-discloses the allegation to DOJ within 120 days of receiving the whistleblower's internal report (and before the DOJ contacts the company); and (2) meets the other requirements for voluntary self-disclosure and presumption of a declination under the Corporate Enforcement and Voluntary Self-Disclosure Policy.[20]

- **Revisions to the DOJ Criminal Division's Compliance Guidance (ECCP)**: In September 2024, DOJ announced revisions to the Criminal Division's compliance guidance, known as the Evaluation of Corporate Compliance Programs (ECCP).[21] With respect to new AI, the updated guidance reflects efforts to analyze how companies are using new technologies in their businesses, and whether that use is accompanied by an appropriate assessment of the potential risks and vulnerabilities that those technologies may present.[22] The revised ECCP additionally emphasized the importance of companies having processes in place to periodically

[15] For more information on the Safe Harbor, *see* our March blog post available here.

[16] The program applies broadly to all corporate misconduct, but specifically identifies certain high priority enforcement areas, including schemes involving financial institutions and the integrity of financial markets; FCPA and FEPA; health care fraud and kickback schemes; federal contract fraud schemes; and domestic corruption schemes. Certain exclusions apply, such as for a tipster who was a CEO, a CFO, or a leader of the scheme; where the tipster has a prior fraud conviction; or where the offense involves crimes of violence. DOJ, "The Criminal Division's Pilot Program on Voluntary Self-Disclosures for Individuals" (April 15, 2024), available here.

[17] *Id.* at 2-3.

[18] DOJ Blogpost, "Criminal Division's Voluntary Self-Disclosures Pilot Program for Individuals" (April 22, 2024), available here.

[19] The amount of the awards will be based on the "net proceeds forfeited," which is the value of forfeited assets remaining after compensating victims and paying other costs associated with the forfeiture. Eligible whistleblowers may receive up to 30% of the first $100 million in net proceeds forfeited, and up to 5% of any net proceeds forfeited between $100 million and $500 million. DOJ Fact Sheet, "U.S. Department of Justice Corporate Whistleblower Awards Pilot Program" (August 1, 2024), available here.

[20] DOJ Temporary Amendment, "Department of Justice Temporary Amendment to Criminal Division Corporate Enforcement and Voluntary Self-Disclosure Policy" (August 1, 2024), available here.

[21] Argentieri Speech, "Principal Deputy Assistant Attorney General Nicole M. Argentieri Delivers Remarks at the Society of Corporate Compliance and Ethics 23rd Annual Compliance & Ethics Institute," (September 23, 2024), available here.

[22] DOJ, "The U.S. Department of Justice Criminal Division Evaluation of Corporate Compliance Programs" (September 23, 2024), available here.

evaluate their own compliance programs, focusing on continuous improvement through the leveraging of data and analytics tools.[23] Furthermore, DOJ will expect companies to incorporate lessons learned from both their own prior misconduct and from issues at other companies into their compliance programs through trainings that are regularly updated and also to focus on evolving risks for the company and the industry in which it operates. Finally, the ECCP incorporated changes related to whistleblower reporting, emphasizing that prosecutors will assess whether companies are promoting whistleblower reports and are assessing employee willingness to report misconduct, such as testing whether employees are aware of and feel comfortable using reporting hotlines.[24]

FCPA

Enforcement of the Foreign Corrupt Practices Act (FCPA) remained a priority in 2024, with the DOJ entering into eight corporate criminal resolutions and issuing one declination under the Criminal Division's Corporate Enforcement and Voluntary Self-Disclosure Policy, which was revised in 2023.[25] The DOJ's actions reflect the continued premium placed on voluntary self-disclosure, as well as proactive and full cooperation. To merit a declination, the DOJ has emphasized the timeliness of the disclosure following the discovery of evidence, as well as the full cooperation and remediation by the company, which included termination of responsible personnel and disgorgement of all ill-gotten gains.[26] The DOJ also continued its increasing cooperation with international authorities, including its first coordinated resolution with Ecuador, two additional resolutions coordinated with South Africa, and continued cooperation with authorities from Brazil, Switzerland, Uruguay, Colombia, Singapore, Portugal and elsewhere.[27]

DOJ also continued securing trial convictions and guilty pleas in a number of significant, high-profile foreign bribery matters in multiple jurisdictions. Among others, the DOJ successfully convicted the former Comptroller General of Ecuador and the former Finance Minister of Mozambique following lengthy trials in Miami and Brooklyn.[28] In addition, DOJ obtained trial convictions in two cases involving former commodities trading executives Javier Aguilar and Glenn Oztemel.[29] Both trials highlighted DOJ's ability to secure and present the testimony of cooperators who plead guilty and testify against their former coconspirators, providing detailed accounts of the bribery schemes. The Aguilar trial included testimony from 10 cooperating witnesses, including the former officials who were bribed, the intermediaries who facilitated the bribe payments, and others.[30] Given these recent successes, DOJ is likely to remain focused on charging individuals in foreign bribery cases.

In addition, the Foreign Extortion Prevention Act (FEPA) was signed into law in December 2023 and amended in July 2024.[31] The FEPA provides a mechanism for U.S. authorities to prosecute the demand side of foreign corruption, and was amended to clarify key jurisdictional hooks as well as the individuals to

[23] *Id.*

[24] *Id.*

[25] Related Enforcement Actions: 2024, U.S. DEP'T of JUSTICE, available here.; In re: Boston Consulting Group, Inc. (CEP Declination Letter) (August 27, 2024), available here.

[26] *Id.*

[27] DOJ Press Release, "Swiss Commodities Trading Company Please Guilty to Foreign Bribery Scheme," (Mar. 28, 2024), available here; DOJ Press Release, "Commodities Trading Company Will Pay Over $661M to Resolve Foreign Bribery Case," (March 1, 2024), available here; DOJ Press Release, "SAP to Pay Over $220M to Resolve Foreign Bribery Investigations," (January 10, 2024), available here.

[28] DOJ Press Release, "Former Comptroller General of Ecuador Sentenced in International Bribery and Money Laundering Scheme," (October 1, 2024), available here; DOJ Press Release, "Former Finance Minister of Mozambique Convicted of $2B Fraud and Money Laundering Scheme," (August 8, 2024), available here.

[29] DOJ Press Release, "Oil and Gas Trader Convicted for Role in Foreign Bribery and Money Laundering Scheme," (February 23, 2024), available here; Press Release, "Former Connecticut-Based Energy Trader Convicted of International Bribery Scheme," (September 26, 2024), available here.

[30] DOJ Press Release, "Ex-Energy Trader for Vitol Convicted of Foreign Bribery and Money Laundering Scheme," (February 23, 2024), available here.

[31] U.S. Congress Bill, "Foreign Extortion Prevention Technical Corrections Act", S. 4548, 118th Cong. (2023), available here.

whom the FEPA applies, in effect harmonizing the law with the FCPA.[32]

The focus on the FCPA and FEPA signals that anti-corruption enforcement is likely to remain active with the incoming administration. FCPA enforcement remained strong under the last Trump Administration and we would expect continued robust enforcement, though the benefits may be even higher for companies that know how to demonstrate that they had strong compliance programs in place.

Digital Assets

Prosecutions related to giants in the digital asset space continued in 2024. The global cryptocurrency exchange BitMEX, for example, pled guilty in July 2024 to violations of the Bank Secrecy Act by failing to establish, implement and maintain an adequate anti-money laundering program.[33] Furthermore, 18 individuals and entities serving as or at cryptocurrency financial services firms were charged in October 2024 for widespread fraud and manipulation in the cryptocurrency markets.[34] In addition, sentences have been handed down related to the breakdown of the FTX exchange, with founder Sam Bankman-Fried sentenced to 25 years in prison and coconspirator sentences ranging from supervised release to seven and a half years in prison.[35]

Financial Institutions

Anti-money laundering enforcement remained strong, with the 10th largest bank in the U.S. pleading guilty and agreeing to pay over $1.8 billion in penalties as a result of the DOJ's investigation into violations of the Bank Secrecy Act and money laundering, marking the first time a U.S. bank pled guilty to conspiracy to commit money laundering.[36] The plea agreement evidences the DOJ's focus on strong compliance programs within the financial institution space.

National Security and Export Controls

In recent years, the DOJ has taken up a renewed focus on national security, sanctions and export controls matters. Beginning in 2022, following Russia's invasion of Ukraine, the DOJ signaled an increased commitment to sanctions enforcement, referring to it as "the new FCPA" in terms of prioritization.[37] In March 2024, Assistant Attorney General Matthew G. Olsen stated that "the National Security Division [will] now interact with corporations and the business community like never before" in this space.[38] In pursuit of such efforts, the DOJ more than doubled the number of prosecutors working on sanctions, export control, and foreign agent registration cases.[39] In May 2024, the National Security Division issued its first declination, to a company that voluntarily disclosed a former employee's scheme to illegally export products to China.[40] As part of its decision not to prosecute, the DOJ cited the timely and voluntary self-disclosure, which came only one week after retaining outside counsel to conduct an internal investigation, as well as the lack of a significant threat to national security posed by the activity and the fact that the company made no unlawful gains from the offense.[41] The DOJ also focused on individual prosecutions under the Foreign Agents Registration Act (FARA), bringing

[32] *Id.*

[33] DOJ Press Release, "Global Cryptocurrency Exchange BitMEX Pleads Guilty To Bank Secrecy Act Offense," (July 10, 2024), available here.

[34] DOJ Press Release, "Eighteen Individuals and Entities Charged in International Operation Targeting Widespread Fraud and Manipulation in the Cryptocurrency Markets," (October 9, 2024), available here.

[35] DOJ Press Release, "Samuel Bankman-Fried Sentenced to 25 Years for His Orchestration of Multiple Fraudulent Schemes" (March 28, 2024), available here; Reuters, "Bankman-Fried's ex-deputy Wang avoids prison time over crypto fraud," Reuters, (November 20, 2024), available here; DOJ Press Release, "Former FTX Executive Ryan Salame Sentenced to 90 Months in Prison," (May 28, 2024), available here.

[36] DOJ Press Release, "TD Bank Pleads Guilty to Bank Secrecy Act and Money Laundering Conspiracy Violations in $1.8B Resolution," (October 10, 2024), available here.

[37] Monaco Speech, "Deputy Attorney General Lisa O. Monaco Delivers Keynote Remarks at 2022 GIR Live: Women in Investigations," (June 16, 2022), available here.

[38] Olsen Speech, "Assistant Attorney General Matthew G. Olsen Delivers Keynote Speech at the American Bar Association's 39th National Institute on White Collar Crime," (March 8, 2024), available here.

[39] *Id.*

[40] In re Sigma-Aldrich, Inc., d/b/a MilliporeSigma, (Declination) (May 14, 2024), available here.

[41] *Id.*

charges against a number of individuals, notably including U.S. Senator Robert Menendez, former New York State official Linda Sun and U.S. Congressman Enrique Roberto "Henry" Cuellar in 2024.[42] Under the Trump Administration, national security is expected to remain a DOJ priority.

Key Takeaways

Following the election, enforcement priorities are likely to shift at both the DOJ and SEC. Based on the last Trump Administration and stated policy preferences, we can predict some priorities:

- The SEC will likely return to more traditional, bread and butter cases that involve harm to retail investors, such as accounting and disclosure fraud, misappropriation of funds by investment advisers, market manipulation and insider trading, and offering frauds. On the other hand, there likely will be a decrease in enforcement activity related to ESG, cybersecurity, off-channel communications and crypto, which were a focus of the SEC under Gensler and the Biden Administration.

- The SEC will levy smaller penalties on large entities, and penalties will need to bear a relation to a measurable benefit the entity received from its alleged securities law violations. The SEC will be less likely to pursue novel theories of disgorgement. The returns on cooperation are likely to be even greater than before, with companies that cooperate with investigations and self-remediate standing to benefit more tangibly than in the past.

- The SEC likely will take a less expansive approach to materiality, will focus more on issuer disclosures directly linked to financial results and less on cyber or ESG issues, and will be less likely to pursue aggressive theories and perceived "regulation by enforcement." With resource constraints likely to continue, the SEC may also shy away from pursuing protracted litigation where they are not assured of success. With the SEC more receptive to the arguments made by public companies and regulated entities, effective, thoughtful advocacy will matter more than ever.

- Under the Trump Administration, some areas of white collar enforcement will continue as priorities or even increase, while others will decline. There is likely to remain a strong focus on FCPA enforcement, which increased during the first Trump Administration. In addition, there is likely to be a continued focus on national security and sanctions/export controls, another area that showed significant activity during the previous Trump Administration. On the other hand, there may be decreased activity in traditional business crimes and in the environmental space. There also likely will be lower penalties and fewer monitorships going forward.

- Most DOJ policies are likely to remain in place, including with respect to corporate compliance and cooperation. Indeed, there may be more potential for reduced penalties or declinations for companies that can point to effective compliance programs, internal investigations and self-remediation in the wake of alleged misconduct. As such, companies should pay particular attention to the state of their compliance programs and ensure that they have engaged in periodic assessments and evaluations of their overall effectiveness, with an emphasis on internal reporting mechanisms, regularly updated trainings and the efficient processing and prioritization of whistleblower complaints. Furthermore, companies should invest in the use of new technologies, as well as data and data analytics tools to enhance their compliance programs, as well as ensure that adequate safeguards are in place to monitor those new technologies.

[42] DOJ, Foreign Agents Registration Act: Recent Cases, available here.

2024 Antitrust Update: Navigating the Evolving Landscape

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

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

Henry Mostyn
Partner
London
hmostyn@cgsh.com

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

Anjali Iyer
Associate
London
aiyer@cgsh.com

Devina Srivastava
Trainee Solicitor
London
dsrivastava@cgsh.com

Antitrust in 2024 was marked by evolving policy developments, vigorous enforcement, and eye-catching court decisions. In the U.S., an aggressive enforcement approach lead to unpredictability and lengthy merger review process across sectors. In the EU, enforcement of the Digital Markets Act (DMA) intensified scrutiny on digital platforms, while a landmark ruling in the *Illumina/GRAIL* matter clarified the scope of the EU Commission's merger jurisdiction. In the UK, the Competition and Markets Authority (CMA) cleared the *Vodafone/Three* merger with behavioral remedies, signaling a significant departure from its historic practice to require structural remedies. 2025 will see new antitrust leadership on both sides of the Atlantic with an expectation that the U.S. will largely return to a more traditional approach on antitrust under the Trump Administration and that Europe will continue to enforce digital rules and bring cases related to AI with a focus on promoting growth in clean tech and AI sectors.

U.S. Antitrust Developments

The U.S. antitrust landscape is likely to experience significant shifts in 2025 due to the change from the Biden to the Trump Administration and to prior changes implemented by the Biden Administration taking effect.

> The Trump Administration is likely to bring increased predictability to antitrust enforcement with a greater focus on bringing traditional cases rather than trying to stretch the law and the facts at least in most areas.

Overall Enforcement Approach

The Biden Administration swung antitrust policy away from a 40-year bipartisan consensus toward a "progressive" approach that was overtly hostile to mergers in general and that viewed previous antitrust enforcement from both parties had been too "lax." With some exceptions related to companies perceived as hostile to conservative priorities—for example, Big Tech platforms accused of conservative censorship—the Trump Administration should swing back toward an antitrust policy that more closely adheres to past practices and antitrust economics.

As a result, the Trump Administration is likely to bring increased predictability to antitrust enforcement with a greater focus on bringing traditional cases rather than trying to stretch the law and the facts, at least in most areas. The Trump Administration could also reduce the burden of investigations by moving away from procedures used by Biden enforcers to increase costs without changing substantive outcomes. Additionally, Trump enforcers are not likely to vilify private equity or continue the Biden Administration's hostility toward using consent decrees to resolve antitrust cases when doing so will protect competition.

That said, the Trump Administration will not necessarily lead to less enforcement overall. Notwithstanding the rhetoric from Biden Administration appointees and credulous press coverage echoing their talking points, in terms of objective measurements of enforcement, such as the number of enforcement actions brought and the percentage of HSR-reported transactions receiving scrutiny, the first Trump Administration was at least as aggressive, if not more so, than the Biden Administration.

The Trump Administration is likely to focus on traditional horizontal merger cases. Enforcement actions in these cases could increase both because the Trump Administration will likely use fewer resources on other types of cases and because Trump enforcers may be more willing to use consent decrees to settle these cases. The Biden Administration largely abandoned the use of consent decrees in settlements, leading to loss in some cases in court that could have been settled and to other mergers going through without action.

Further, the Trump Administration is less likely to pursue "edge" theories in merger cases, including for example aggressive vertical theories, conglomerate effects theories such as cases based on bundling, or potential competition cases. The Trump Administration is also less likely to target specific individuals in merger cases, while the Biden Administration, in a questionable use of antitrust law, forced some merging companies to agree to bar individuals from serving as officers or directors of merged companies as a condition to approving the merger based on alleged antitrust concerns with those individuals' prior conduct.

The Trump Administration is also less likely to pursue controversial initiatives such as the FTC's attempt to resurrect the Robinson-Patman Act's limitations on price discrimination, which lack a sound basis in antitrust economics and prior to the Biden Administration were dead-letter for decades.

In addition, the Trump Administration is less likely than the Biden Administration to aggressively use antitrust laws to regulate broad swathes of the economy as opposed to engaging in case-by-case adjudication. In particular, the Biden FTC sought to promulgate rules that banned non-competes in employment contexts. The courts have blocked these rules from going into effect, and the Trump Administration will likely end this rulemaking. As another example, the Biden Administration suggested antitrust law has a significant role to play in regulation of artificial intelligence, while the Trump Administration likely will take a less interventionist approach and allow the competition to occur in the market. For further discussion, *see* Non-Competes: One Step Forward and Two Steps Back.

To be sure, the Trump Administration is likely to continue some of the Biden Administration's initiatives. In particular, the "Big Tech" cases will likely continue. President Trump has said as much explicitly, and Vice President Elect JD Vance and prospective appointees have made similar statements. Indeed, several currently pending cases against Big Tech companies were initiated under the first Trump Administration, not the Biden Administration, including the Google case that is now in the remedy phase and the FTC's challenge to Meta's acquisitions of Instagram and WhatsApp. The Trump Administration could also add a new flavor to the Big Tech cases by investigating alleged coordination among Big Tech firms to censor "disinformation" and to de-platform conservatives and other unpopular voices.

This increasing politicization of antitrust could also manifest in the Trump Administration using the antitrust laws against coordinated action on social goals such as "green" initiatives or DEI. Congressional Republicans have for several years been alleging that companies violated the antitrust laws by agreeing, for example, on net zero goals, and Trump's prospective appointee as FTC Chair has specifically called out these issues as ones that the FTC should pursue. Thus, while the Biden Administration sought to use the antitrust laws to advance its political goals—*e.g.*, by attacking private equity firms—the Trump Administration might do the same in a different direction. That represents a worrying trend where antitrust priorities are dictated by political goals that swing from administration to administration rather than by more objective values such as protecting free market competition and increasing consumer welfare.

Leadership Changes at FTC and DOJ

The leadership at the FTC and DOJ Antitrust Division will change in the Trump Administration.

At the FTC, President Trump has announced that he will designate Andrew Ferguson, currently one of two Republican Commissioners, as FTC Chair. Trump can make that designation immediately. In a number of dissenting statements while Commissioner and in lobbying for the position as Chair, Ferguson has made clear that he is opposed to the FTC's most aggressive theories and abuses of process, while also making clear that he will be a Trump loyalist who supports, for example, action against Big Tech for censorship and de-platforming. Once appointed, Ferguson will name new heads of the Bureau of Competition and Bureau of Economics to run the day-to-day antitrust-related operations of the FTC. Trump will also appoint a replacement for current Chair Lina Khan, likely Mark Meador, an antitrust lawyer who recently served as counsel on antitrust policy to the Senate Judiciary Committee. Whether the changes in leadership will help to restore FTC staff morale, which fell precipitously under Khan from the high levels under the prior Trump Administration, is unclear.

At the DOJ Antitrust Division, Assistant Attorney General Jonathan Kanter resigned in December 2024. President Trump has announced that he will appoint Gail Slater as the new Assistant Attorney General, although Senate confirmation will take time. Slater was most recently economic advisor to Vice President-Elect JD Vance and previously worked in the prior Trump Administration on the National Economic Council, in the private sector at Fox and Roku, and at the FTC, including as a staffer to Democratic FTC Commissioner Julie Brill. In announcing the nomination, President Trump emphasized that the Antitrust Division

would continue to pursue cases against "Big Tech." Apart from that focus on Big Tech, Slater is likely to adopt a more traditional approach to antitrust than Kanter. In practice, the transition to new leadership at DOJ Antitrust is likely to occur prior to Slater's confirmation: traditionally, a senior career DOJ official will temporarily run the Antitrust Division and then a new Principal Deputy Assistant Attorney General, a political position that does not require Senate approval, is installed to serve as Acting AAG.

HSR Changes, Merger Guidelines, and Other Guidelines

The Biden Administration adopted revised Hart-Scott-Rodino (HSR) rules for pre-merger filings. These rules will impose significantly more burden on HSR filers without much justification. The two Republican Commissioners voted in favor of these rules, seemingly as a compromise so that the three Democratic Commissioners would drop the most extreme parts of their original proposal. The new rules are now embedded as formal federal regulations and scheduled to go into effect on February 10. The rules cannot be withdrawn administratively without a new rulemaking process, which would likely take at least a year, although there is some chance that Congress could strike them down under the Congressional Review Act. Regardless, the Trump Administration could adopt a more reasonable and practical approach to implementing the new rules than what would have been likely under the Biden Administration, potentially lessening the additional burden.

The Biden Administration also withdrew the long-standing 2010 merger guidelines and in December 2023 issued a new set of merger guidelines that largely ignored recent case law and antitrust economics. The Trump Administration could withdraw these guidelines or significantly revise them, and could potentially return to an approach in practice more like the 2010 approach.

The Biden Administration also withdrew a number of other long-standing guidelines, including about competitor collaborations and information sharing, yet did not replace them with anything new. These guidelines summarized the law in a neutral way and helped provide guidance to businesses about what the antitrust laws require. Their withdrawal increases uncertainty for business, and the Trump Administration could potentially develop new guidelines to provide better guidance to business.

Conclusion

The Biden Administration attempted to implement a major shift in the U.S. approach to antitrust. The anticipated return to a more traditional approach under the Trump Administration hopefully will lead to more reasonable enforcement for the next four years in most areas. However, the increased politicization of antitrust by the Biden Administration could also continue under the Trump Administration, just with different targets, which is a worrying development for antitrust enforcement going forward.

Europe and ROW Antitrust Developments

In 2024, Europe and the ROW saw increasing scrutiny of digital platforms via new digital regulation; a landmark ruling that clarified the EU's merger jurisdiction; a stepchange in how the UK approaches behavioral remedies in mergers; and increasing scrutiny of AI partnerships. In 2025, we expect the new EU Commission to continue to enforce digital rules, to adapt its approach to below-threshold mergers and to bring cases in relation to AI. In a leadership shift, Teresa Ribera will succeed Margrethe Vestager, as EU Competition Commissioner, and will also take up the role of Executive Vice-President for a Clean, Just and Competitive Transition. Ribera's portfolio echoes the recent Draghi report[1] on European competitiveness, and her broad aim will be to "unlock investment, create lead markets for clean tech and put in place conditions for companies to grow and compete."

[1] European Commission, "The future of European competitiveness: Report by Mario Draghi" (updated September 9, 2024), available here.

Digital Regulation Comes Into Force in the EU, and Is Passed in Japan and the UK

In 2024, the obligations under the EU's DMA, prescribing a series of "dos and don'ts" for the largest tech-companies or gatekeepers, became effective. So far, seven companies have been designated as gatekeepers: Alphabet, Amazon, Apple, Booking.com, ByteDance, Meta and Microsoft.

The EU Commission has been actively looking to enforce the new rules, launching investigations into Alphabet, Apple and Meta, purporting to address issues such as self-preferencing in ranking, app distribution on mobile OSs and the right way to display user choice screens. The Commission issued preliminary findings against Apple in relation to its anti-steering policies in the App Store,[2] and to enforce interoperability obligations between iOS/iPadOS and connected devices.[3]

Across the English Channel, the UK adopted similar legislation to the DMA with its own Digital Markets, Competition, and Consumer Act. The UK approach also seeks to impose specific obligations on a handful of digital platforms (which it calls firms with "strategic market status" or SMS), but seeks to take a more flexible approach where the UK agency will devise codes of conduct tailored to specific firm activities, and to explicitly consider consumer benefits in all aspects of its enforcement. In 2025, the new regime will come into force, with the first SMS firms being designated and codes of conduct imposed. The open question for firms and businesses is whether the UK will mostly seek to mimic the enforcement in the EU under the DMA or will try to forge its own path.

Beyond the EU and the UK, 2024 saw a step up in proposals for regulation of digital platforms. In Japan, the Smartphones Act was adopted, which imposes similar obligations to the DMA but focused on mobile platforms. Platform legislation was also proposed in Australia, India and Turkey.

In 2025, many of these regimes will come into force and tech firms and businesses will need to be cognizant of the "similar but different" rules that apply in each jurisdiction. Our regularly-updated Digital Markets Regulation Handbook, available here, can help firms navigate the evolving landscape.

Illumina/GRAIL: ECJ Rules European Commission Lacks Jurisdiction to Review Merger Falling Below EU and National Merger Thresholds

On September 3, 2024, the Court of Justice delivered a landmark judgment in *Illumina/GRAIL*, by ruling in favor of Illumina in its challenge to the EC's unprecedented assertion of jurisdiction over a transaction that met no notification thresholds at either EU or Member State level.[4] Cleary Gottlieb acted for Illumina in the case.

In a nutshell, the judgment finds that the EU's policy of seeking to review non-reportable transactions based on a re-interpretation of Article 22 of the EU Merger Regulation is unlawful. A Member State with domestic merger control rules cannot seek an Article 22 referral if the transaction does not fall within its national merger control rules.

The judgment has significant implications for companies because it limits the main direct avenue the EC intended to use to scrutinize concentrations falling below both EU and national merger control thresholds. Unless a transaction is reviewable based on national merger control rules, an EU Member State will no longer be able to request that a case be referred to the EC.

[2] European Commission, "Commission sends preliminary findings to Apple and opens additional non-compliance investigation against Apple under the Digital Markets Act" (June 24, 2024), available here.

[3] European Commission, "Commission starts first proceedings to specify Apple's interoperability obligations under the Digital Markets Act" (September 19, 2024), available here.

[4] For more information, see our September alert memo available here.

Member States may continue to take action to bring more mergers within the purview of their national merger control rules.

In 2025, the Commission will need to assess how to respond to the judgment. In the short term, the Commission may consider pivoting to applying abuse of dominance rules (as in the recent Towercast case[5]), although that is limited to acquirers that hold a dominant market position. In parallel, Member States may continue to take action to bring more mergers within the purview of their national merger control rules, which the Commission may in turn then try to review via Article 22. However, in line with the ECJ judgment, if the Commission wants to review more transactions at the EU level, it will have to seek a revision of the EU Merger Regulation's notification thresholds.

The UK Signals a Shift in Approach Behavioral Remedies in the Vodafone/Three Merger

The UK in 2024 also saw a notable merger decision that may have implications for companies looking to do deals in 2025. In early December, the UK Competition and Markets Authority (CMA) cleared the *Vodafone/Three* merger, subject to binding commitments. Taken together with recent announcements by the CMA's CEO, Sarah Cardell, this decision suggests a shift in UK merger control towards a more permissive enforcement environment.

- The CMA has cleared the merger of two major UK mobile telecommunications operators. This represents a significant change from the CMA's position in 2016, when it supported the EU Commission's prohibition of a similar tie up between O2 and Three.
- The CMA has accepted a novel investment commitment combined with short-term customer protections, including time-limited price controls. This is a significant development in UK merger control, because it represents a departure from the CMA's usual preference to impose structural remedies (*i.e.* divestitures) or otherwise block problematic deals. Top CMA officials have been outspoken against behavioral remedies in recent years, and the CMA has rejected such remedies in favor of divestitures in several recent cases.

The decision follows indications that the new UK Labour Government was steering the CMA to pursue a less dogmatic approach to merger control consistent with the Government's pro-growth agenda. In October this year, the UK Government promised to "rip up the bureaucracy that blocks investment," encouraging regulators, including the CMA, to "take growth seriously."[6]

In response, the CMA has signaled a change in its approach to merger review. Last month, Sarah Cardell announced[7] a review in the agency's approach to merger remedies that will include considering when behavioral remedies may be appropriate, the scope for remedies that lock in rivalry-enhancing efficiencies and preserve customer benefits, and ways to move to remedy discussions "as quickly as possible" in merger investigations. This case is the first example of this new approach in practice.

Increasing Scrutiny of AI Partnerships

Across Europe and ROW, agencies are increasingly scrutinizing AI and, in particular, AI partnerships. The UK's CMA concluded its review of four AI partnerships in 2024, and cleared three of them (*Amazon/Anthropic*, *Alphabet/Anthropic*, and *Microsoft/Mistral*) because

[5] The *Towercast* judgment made clear that the EC may challenge concentrations *ex post* under general antitrust provisions, notably Article 102 TFEU, irrespective of the existence of a dedicated EU merger control regime, Case C-449/21 *Towercast*, Judgment of 16 March 2023.

[6] UK Government Press Release, "Major investment deals set to be announced at government's inaugural International Investment Summit as PM vows to 'remove needless regulation' declaring Britain open for business" (October 14, 2024), available here.

[7] Sarah Cardell, "Driving growth: how the CMA is rising to the challenge" (November 21, 2024), available here.

the UK lacked jurisdiction. For the fourth transaction (*Microsoft/Inflection*), the UK asserted jurisdiction but cleared the deal as not giving rise to competition concerns.

For 2025, companies need to be aware that regulators are likely to take an increasingly expansive approach to jurisdiction when it comes to AI partnerships. They need to be aware from an early stage of the antitrust concerns around AI, and consider building into their governance framework the three core principles promulgated by the U.S., EU and UK agencies of fair dealing, interoperability and choice.[8]

[8] European Commission, UK Competition and Markets Authority, U.S. Department of Justice, U.S. Federal Trade Commission, "Joint Statement of Competition in Generative AI Foundation Models by EU Commission" (July 23, 2024), available here.

Outlook for M&A and Activism in 2025

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

Kimberly R. Spoerri
Partner
New York
kspoerri@cgsh.com

Predictions for M&A in 2025

The Overall M&A Environment

Many have predicted an M&A boom in 2025 and recent CEO surveys exhibit rising confidence. Psychology is as important to the merger market as any human endeavor, so one should not discount the power of renewed optimism to be a self-fulfilling prophecy. We expect reality to be more nuanced, however, although 2025 should be a strong year (the usual caveats about fiscal and macro uncertainty aside).

On the corporate side, as in recent years, portfolio reshaping and de-conglomeration will remain a significant driver of transactions, as the market continues to reward simplicity and focus. We also expect elevated interest in cross-border transactions into the U.S. from European corporates looking for greater exposure to the higher-growth U.S. market.

Ultimately, however, private equity will need to be a key driver of the rebound.

Private Equity Outlook is More Optimistic, but Mixed

Sponsors continue to sit on significant dry powder and a record backlog of portfolio companies to exit. Buy-side activity began to recover in 2024 as interest rates moderated, but with financing costs remaining elevated and valuation gaps lingering, unless and until interest rates recede further we expect to see a continued "barbell" effect in the market in the near term, with both high quality and distressed assets

Buy-side activity began to recover in 2024 as interest rates moderated, but with financing costs remaining elevated and valuation gaps lingering, unless and until interest rates recede further we expect to see a continued “barbell” effect in the market in the near term.

seeing strong interest from private equity bidders while activity is more mixed in between.

Meanwhile, as the exit backlog has mounted, limited partners are increasingly focused on distributions to paid-in-capital and sponsors are eager to deliver. Sponsors have continued to utilize alternative liquidity options, new and old—minority stakes sales, continuation funds, GP-led secondaries, dividend recapitalizations, and NAV loans—while holding assets in their portfolio. While these alternative liquidity options aren’t going anywhere, there are limits to their ability to compensate for the shortfall in traditional exits, which sponsors will be anxious to increase in order to return capital and boost further fundraising. An increase in sponsor-to-sponsor transactions will be needed to clear the backlog, however, and this is where buy-side and sell-side challenges converge.

We will see a shift, but not a sea change, on the approach to antitrust risk.

Lina Kahn may be gone, but we don’t expect parties to throw caution to the wind on antitrust risk any time soon, despite much commentary that the regulatory reins are set to loosen.

First, as we have noted elsewhere in this memorandum, the first Trump Administration was at least as aggressive, if not more so, than the Biden Administration in overall levels of enforcement. What distinguished the agencies under Biden has been the unpredictability of enforcement activity, more novel theories of harm, and resistance to consent decrees. A return to predictability and the willingness of agencies to settle merger challenges should increase risk appetites and open up some bigger bets, but the degree to which those conditions will return, and the overall level of scrutiny, remains a significant open question.

Second, the recent history of merger litigation has exposed the potential limitations of “hell or high water” and other similarly strong regulatory covenants, as targets seeking to enforce these covenants have encountered difficulties in doing so in a timely manner. This, together with agency behavior, led to a focus on “fix it first” strategies and a surge in the use of antitrust reverse termination fees since 2020, with targets looking to financial pain to condition buyer behavior. We expect target boards and sellers to continue to pay heightened attention to antitrust risk and approval strategy, and to seek termination fees at elevated rates. Buyers, on the other hand, should still proceed with caution in negotiating antitrust covenants and termination fees.

Shareholder Activism in 2025

2024 was once again a robust year for activism and 2025 will be no different.

Many key themes of the activism landscape in 2024 were extensions of trends from years prior. These include the continued diversification of the activist field (with additional new and spinoff players joining the established firms), an elevated focus on strategic and operational campaigns and increased targeting of CEOs. After three relatively frenetic years of activism post-pandemic, however, it is worth stepping back to observe the macro trends that have taken shape.

The profusion of activists and extended legacy of activism in the U.S., together with companies increasingly becoming their own activists or adopting more of the private equity playbook, has resulted in a larger pool of activists reaching for a dwindling supply of attractive targets. This has contributed to two significant recent phenomena:

- The so-called activist "swarm"—with companies frequently facing two or three (or more) activists in the same campaign season. This itself has contributed to one of the more significant developments in activist tactics—the rise of the "sneak attack", as activists seeking to preempt the pack are increasingly willing to forego private engagement and initiate campaigns publicly.

- The exportation of U.S.-style activism abroad, which is not limited to U.S. activist funds but heavily influenced by them, as they seek opportunities in the less-crowded waters outside the U.S. Traditional barriers to activism in these other jurisdictions—whether from more consolidated share ownership or regulatory regimes—have become less of a deterrent. Activists are willing to run campaigns even when the odds may seem stacked against them, and argue that the results (even if not a win at the ballot box) signify a sufficient mandate for change. (An attitude which may also reverberate stateside, with activists being more willing to take on controlled companies.)

The profusion of activists and extended legacy of activism in the U.S., together with companies increasingly becoming their own activists or adopting more of the private equity playbook, has resulted in a larger pool of activists reaching for a dwindling supply of attractive targets.

In the U.S., the increase in campaigns initiated publicly only increases the importance of advance preparation. It is no longer sufficient to have a "break glass" plan. Companies need to conduct a more detailed assessment of vulnerabilities, consider proactive steps if consistent with the board's strategy, develop more sophisticated rebuttals and media response plans and revisit each of these more regularly. This also applies to recently spun-off or IPO'ed companies, as activists are giving these issuers less runway than they have in years past. As a result of more sophisticated advance preparation, as well as increasing familiarity with the universal proxy landscape, we expect to see more companies being less quick to settle.

Outside the U.S., it is only a matter of time before U.S.-style settlements become more common, although we believe local dynamics will continue to keep settlement rates much lower than what is seen in the U.S. for the foreseeable future.

FDI Review Regimes Ramp up Globally and Enhance Enforcement; U.S. Outbound Investment Regime Goes into Effect

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

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

Alexi T. Stocker
Associate
Washington, D.C.
astocker@cgsh.com

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

In 2025, boards of directors face a well-established and active global foreign direct investment (FDI) landscape where regulatory review continues to expand and develop. Last year, the Committee on Foreign Investment in the U.S. (CFIUS) issued a final rule enhancing its mitigation and enforcement authority. Non-U.S. FDI review regimes, particularly in Europe, have become more active, with a number of new regimes entering into effect and an increasing number of transactions subject to regulatory scrutiny. The European Commission proposed a new EU-wide FDI Screening Regulation in March 2024, which aims to overhaul the existing EU FDI regime. As concern grows over access to and control over artificial intelligence (AI), semiconductors and other advanced and critical technologies, FDI approvals have become a significant regulatory issue for many cross-border transactions.

The European Commission proposed a new EU-wide FDI Screening Regulation in March 2024, which aims to overhaul the existing EU FDI regime.

On January 2, 2025, the long-awaited U.S. Outbound Investment Security Program (the Program) became effective. Under the Program, U.S. persons are prohibited from engaging in, or required to notify the U.S. Department of the Treasury (Treasury) regarding, a broad range of transactions involving entities engaged in certain activities relating to semiconductors and microelectronics, quantum information technologies and AI systems in "countries of concern" (presently limited to China, Hong Kong and Macau). In early 2024, the European Commission began a consultation and assessment process for developing an outbound investment review program focused on the risk of leakage of "emerging and sensitive technologies," and plans to publish a proposed policy response towards the end of 2025.

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 and strategic acquisitions.

We highlight below major 2024 developments relating to certain key FDI review regimes:

- **U.S.** In December 2024, two new rules went into effect expanding CFIUS's enforcement authority. First, the Treasury issued a final rule that expands CFIUS's ability to review certain real estate transactions by foreign persons near listed military bases and installations. The final rule adds 59 military bases and installations to the existing list and expands CFIUS's jurisdiction to review certain real estate transactions near eight military bases and installations on the existing list. This rule came on the heels of the Biden administration's May 2024 order requiring a company majority owned by Chinese nationals to divest land—which was not notified to CFIUS when acquired, but subsequently investigated by CFIUS following a tip—near a Wyoming military base.[1] Second, Treasury issued a final rule that modified and expanded CFIUS's mitigation and enforcement authority. The rule enhanced CFIUS's authority by expanding CFIUS's authority to investigate non-notified transactions; strengthening CFIUS's subpoena power, including in connection with the review of non-notified transactions; requiring transaction parties to substantively respond to mitigation proposals within three business days; and expanding CFIUS's authority for civil monetary penalties, including increasing the maximum penalties for failing to make mandatory filings, violating material provisions of mitigation agreements and making material misstatements and omissions outside of an active CFIUS review (such as during monitoring and compliance periods).

- **European Union**. On January 24, 2024, the European Commission proposed a new EU FDI Screening Regulation. If adopted by the European Parliament and Council, the new regulation would (1) make investment screening compulsory in the EU, (2) harmonize procedural rules and expand the scope of investment screening, (3) reaffirm and clarify substantive analysis guidelines and (4) reinforce cooperation between enforcement authorities through ten key changes to the existing regime.[2] Adoption of the new regulation is not expected until 2027 at the earliest. On October 17, 2024, the European Commission published its fourth annual report on the screening of foreign direct investments into the EU.

[1] For additional details, see our May blog post available here.

[2] For additional details, see our March alert memo available here.

As of this writing, 22 of 27 EU member states have an active FDI regime. Ireland's FDI regime went into effect on January 6, 2025 (after several delays), and the remaining four member states are expected to join the FDI block over the course of 2025. The number of filings undergoing screening within the EU FDI screening cooperation mechanism increased in 2024, continuing the upward trend from prior years.[3]

- **United Kingdom**. The UK FDI review regime has been in effect for approximately three years. In May 2024, the UK government published updated guidance on the application of the National Security and Investment Act and updated the policy statement in which it sets out the factors that the Secretary of State expects to use when deciding whether to exercise its power to "call in" transactions for full national security review.[4]

- **Singapore**. In January 2024, Singapore's Parliament passed the Significant Investments Review Act, which went into effect in March 2024 and implements a limited FDI regime whereby foreign investment into "designated entities"—Singaporean companies on an enumerated list—are subject to notification or approval requirements, depending on the level of control acquired.

Outbound Investment Regimes Commence

As noted above, in October 2024, Treasury issued a Final Rule implementing the Program. Under the Final Rule, U.S. persons will be prohibited from making or knowingly directing, or required to notify the U.S. government regarding, certain investments in entities engaged in certain "covered activities" relating to semiconductors and microelectronics, quantum information technologies and artificial intelligence in "countries of concern" (presently defined to include just China, Hong Kong and Macao). Although previously referred to informally as "Reverse CFIUS" in industry circles, the Program does not contemplate a case-by-case review of outbound investments. Instead, the Program will require parties to determine whether a given transaction is either prohibited, subject to notification or permissible without notification, which would require parties to determine whether (1) a "U.S. person" is making or knowingly directing (2) a "covered transaction" with (3) a "covered foreign person"—namely, a "person of a country of concern" engaged in certain defined activities involving "covered activities." Each of those terms is defined in the final rule.

If outbound investment policies similar to that of the U.S. Outbound Investment Security Program are proposed and adopted, such policies could further complicate investments by U.S., UK and EU persons in certain Chinese industries.

In January 2024, the European Commission issued a White Paper on outbound investment control. The White Paper noted that neither the dual-use export control system nor the EU FDI Regulation (nor the domestic FDI regimes) govern outbound investments, which entail the risk of leakage of "emerging and sensitive technologies." The White Paper in turn kicked off a consultation and assessment phase, which will culminate in a summer 2025 risk assessment of the EU Member States' monitoring and review of certain outbound investments, and an autumn 2025 publication of the European Commission's assessment and proposal for a policy response.[5] And in April 2024, the United Kingdom likewise indicated that it is considering more substantive changes to the rules on outward investment, following in the footsteps of the U.S. and EU.[6] If outbound investment policies similar to that of the U.S.

[3] For additional details, see our November alert memo available here.

[4] For additional details, see our May blog post available here.

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

[6] While the UK National Security and Investment Act nominally applies to outward investment in some circumstances, the UK Government stated in April 2024 that it would "launch a dedicated analytical team to deepen understanding of potential risks of outward investment in sensitive sectors." *See* Cabinet Office, "Press release: Deputy Prime Minister to boost economic defences against threats to British economic model" (April 18, 2024), available here.

Outbound Investment Security Program are proposed and adopted, such policies could further complicate investments by U.S., UK and EU persons in certain Chinese industries.

Given the consequences that FDI review regimes can have for cross-border transactions, and the implications of new 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.[7] 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, companies that collect and maintain sensitive (including personal) information and companies with government relationships) or companies with ties to China and other possible "countries of concern," like Russia and Belarus. Management should also be directed to consider 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.

[7] 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.

A New Regulatory Environment for Climate and Other ESG Reporting Rules

Amélie Champsaur
Partner
Paris
achampsaur@cgsh.com

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

Shuangjun Wang
Partner
New York
shwang@cgsh.com

Léa Delanys
Associate
Paris
ldelanys@cgsh.com

The Ill-Fated SEC Climate Rule

On March 6, 2024, the SEC adopted final rules "to enhance and standardize climate-related disclosures for investors," which included, among other things, requirements to disclose material climate-related risks and related governance policies and practices and mitigation and adaptation activities, targets and goals, Scope 1 and 2 emissions reports and financial statement effects of severe weather events and other natural conditions, including related costs and expenditures (the Climate Rule).[1] Almost immediately upon release of the Climate Rule, multiple lawsuits were filed in federal court objecting to the rule on multiple bases, including that the rule is arbitrary and capricious under the Administrative Procedure Act, the rule exceeds the SEC's statutory authority and the rule violates the First Amendment by compelling political speech.[2] The U.S. Court of Appeals for the Eighth Circuit was randomly selected as the venue for consolidating the nine filed lawsuits and on April 4, 2024 the SEC voluntarily stayed the rules pending the outcome of the litigation. Briefs have been filed by all parties and the case is currently pending a hearing date.

---

1 SEC Press Release, "SEC Adopts Rules to Enhance and Standardize Climate-Related Disclosures for Investors" (March 6, 2024), available here. SEC Final Rule, "The Enhancement and Standardization of Climate-Related Disclosures for Investors" (March 2024), available here.

2 While eight of the lawsuits followed similar arguments, one filed by environmental groups represented by Earthjustice argued that the SEC's action was arbitrary and capricious under the Administrative Procedure Act because it did not include all the elements in the proposed rule, including the requirement to disclose Scope 3 emissions, and that the SEC was not mandating disclosure that investors required to make informed investment decisions.

Recently, the Fifth Circuit has vacated multiple SEC and Department of Labor rules related to climate and ESG matters on the basis that they were arbitrary and capricious under the Administrative Procedures Act, most recently, the SEC's approval of a Nasdaq rule requiring most listed companies to disclose the gender and racial/ethnic makeup of their boards of directors, or disclose why they do not, based on a finding that the SEC failed to justify its determination that Nasdaq's rule was consistent with the requirements of the Exchange Act. *See* Alliance for Fair Board Recruitment; National Center for Public Policy Research v. Securities and Exchange Commission (December 11, 2024), available here.

Companies will need to consider how to prepare and comply with applicable rules, while at the same time facing divided stakeholders, including those who are increasingly vocal and skeptical of the value of climate and other ESG-related reporting.

On December 4, 2024, President-elect Donald Trump announced that Paul Atkins would be his nominee to the SEC as Chairman. Current Chair Gensler and Commissioner Lizárraga both announced their intentions to step down in January 2025 before the inauguration, meaning the SEC will have a majority of Republican Commissioners even before Atkins can be confirmed. The change in administration is expected to bring a deregulatory focus and anticipated reduction in budget and spending for administrative agencies, which, together with the quick turnover at the SEC, is anticipated to mean the end of certain ESG related SEC rulemaking initiatives, including the Climate Rule (along with any new proposed rules on board diversity disclosure and human capital management reporting). Procedurally, the SEC under the new administration could abandon the defense of the rule in court (leading to its vacatur); alternatively, it could take regulatory action to rescind the rule (which would require formal rulemaking, including new notice and comment periods), and, pending a final determination, the SEC could announce that it will not lift the stay or enforce the rule, so that in practice it is never implemented.

While the Climate Rule is assumed to be dead, other climate-related reporting regulations applicable to many U.S. companies will continue to take effect, including the Directive (EU) 2022/2464, as regards corporate sustainability reporting (the CSRD) in Europe and California's climate reporting laws. Companies will need to consider how to prepare and comply with applicable rules, while at the same time facing divided stakeholders, including those who are increasingly vocal and skeptical of the value of climate and other ESG-related reporting.

The EU and the Corporate Sustainability Reporting Directive

CSRD entered into force on January 5, 2023.[3] The main objective of the CSRD is to harmonize companies' sustainability reporting and to improve the availability and quality of ESG disclosures. The CSRD requires sustainability reports describing risks, opportunities and impacts, including transition plans material to a company's business model and strategy relating to a broad range of environmental, social and human rights and governance factors. For example, with respect to environmental factors, the CSRD goes beyond climate and covers general cross-cutting disclosures, as well as pollution, water resources, biodiversity, circular economy, workforce, affected communities, end-users and business conduct. The materiality disclosure threshold is based on a "double materiality" standard, which, unlike the U.S. securities law concept of materiality, requires disclosure both when ESG factors materially impact the financial performance of a company (financial materiality) and when the company's activities materially impact society and the environment (impact materiality). In-scope companies include not just EU-domiciled and -listed companies but also large EU subsidiaries[4] of companies outside the EU (third-country companies) and third-country companies with significant EU market activity.[5,6]

While additional implementing standards are still forthcoming, on August 7, 2024, the European Commission published a set of Frequently Asked Questions (FAQs)[7] on the CSRD, providing some

[3] As a directive, the CSRD must be transposed into national law by Member States, as a result of which there may be slight differences from one Member State to another where the CSRD leaves room for discretion.

[4] In-scope subsidiaries include EU domiciled subsidiaries that meet two of three thresholds including (i) 250 employees over the financial year, (ii) a net turnover of €40 million and (iii) a balance sheet of over €20 million, whether on a solo or a consolidated basis.

[5] In-scope companies include third-country companies with an EU net turnover of more than €150 million and an EU subsidiary, or, in the absence of such a subsidiary, an EU branch with a net turnover of more than €40 million.

[6] For details on CSRD scope and applicability to companies, see our February 2023 alert memo available here.

[7] European Commission, "Frequently asked questions on the implementation of the EU corporate sustainability reporting rules" (August 7, 2024), available here.

information for how third-country companies will be required to report:[8]

- For third-country parent reporting, an EU subsidiary or branch of an in-scope third-country group will be required to publish and make accessible group level sustainability information. The content of this sustainability report will be more limited compared to the sustainability statement to be provided by EU companies and large EU subsidiaries.
- A third-country parent will be able to voluntarily publish the group level report ahead of the 2029 reporting date, thereby exempting its large EU subsidiaries,[9] provided that this group level sustainability reporting meets the standards applicable to the EU subsidiaries or equivalent standards.
- While CSRD reporting for EU companies will be required as part of the consolidated management report, *i.e.*, annual report, a third-country company consolidated sustainability statement can be included in a separate document from the annual report.
- A large EU subsidiary whose parent is a third-country company will be permitted to prepare and publish a consolidated sustainability statement that includes all EU companies that are direct or indirect subsidiaries of the third-country parent through the fiscal year ending on or before January 6, 2030. This "sister company" exemption means that large EU subsidiaries will be permitted to report together rather than on an individual basis through fiscal year 2029 (for December 31 fiscal-year-end companies).
- A third-party assurance opinion will be required on the sustainability report.
- As a Directive, the CSRD needs to be transposed in each Member States to become fully applicable. National transpositions may impose greater requirements on companies, including lower thresholds, and thus applicable national transpositions will need to be reviewed and confirmed. As of this publication, ten Member States, including Germany, Luxembourg and the Netherlands, have not yet transposed the CSRD.

Even though voluntary reporting by third-country company groups is permitted in lieu of large EU subsidiary reporting, since reporting standards for third-country companies have not yet been published, many non-EU groups are considering whether to report on behalf of the large EU subsidiaries in the first instance. Any decision on when to move to consolidated group reporting should take into consideration company structure, including the number of large EU subsidiaries, the ability to utilize "sister company" reporting and the difficulty in preparing data for reporting for EU subsidiaries or the consolidated group. It will also depend on the content of future sustainability reporting standards for third-country groups and the extent to which they differ from the standards applicable to EU companies.

Recent announcements from the European Commission suggest ongoing work to prepare an "omnibus" directive aimed at consolidating and rationalizing the broader EU ESG reporting framework (including the CSRD, the Corporate Due Diligence Directive (CSDDD) and the Taxonomy Regulation).

California Climate Reporting Mandates

In 2023, California adopted three laws related to climate reporting (the CA Climate Rules). The first two, SB-253 (the Climate Corporate Data Accountability Act) and SB-261 (the Climate-Related Financial Risk Act), apply to all public and private companies that "do business in California" (CA Covered Entities).

[8] European Union, "Commission Notice on the interpretation of certain legal provisions in Directive 2013/34/EU (Accounting Directive), Directive 2006/43/EC (Audit Directive), Regulation (EU) No 537/2014 (Audit Regulation), Directive 2004/109/EC (Transparency Directive), Delegated Regulation (EU) 2023/2772 (first set of European Sustainability Reporting Standards, 'first ESRS delegated act'), and Regulation (EU) 2019/2088 (Sustainable Finance Disclosures Regulation, 'SFDR') as regards sustainability reporting," available here.

[9] Large EU-listed companies cannot benefit from the parent company exemption.

SB-253 requires CA Covered Entities with total annual revenues in excess of $1 billion to publicly disclose Scope 1 and 2 emissions starting in 2026 and Scope 3 emissions starting in 2027, and to obtain assurance on such data from an independent third-party. On December 5, 2024, the California Air Resources Board (CARB) published an Enforcement Notice that allows companies to use existing reporting systems and data collected for Scope 1 and 2 emissions disclosures for the first reporting cycle, and assured that "CARB will not take enforcement action for incomplete reporting against entities, as long as the companies make a good faith effort to retain all data relevant to emissions reporting for the entity's prior fiscal year."[10] Additional specific requirements and guidance will be published by CARB in due course. SB-261 requires CA Covered Entities with total annual revenues in excess of $500 million to prepare biennial reports beginning on or before January 1, 2026 disclosing the company's climate-related financial risk and the measures the company has adopted to reduce and adapt to such climate-related financial risk.

Like the SEC Climate Rule, SB-253 and SB-261 are subject to legal challenge. Chamber of Commerce of the United States of America et al. v. California Air Resources Board et al. challenges the laws on the basis that they are unconstitutional for violating the First Amendment. On November 5, 2024, the U.S. District Court for the Central District of California deferred a plaintiff motion for summary judgment and allowed the challenge to move into discovery. Given an expected lengthy time for discovery and any further motions or trial, in scope companies should continue to prepare for compliance on the current timeline.

The third law, AB 1305 (the Voluntary Carbon Market Disclosures), requires disclosure of voluntary carbon markets, sales and purchases in or from California and website disclosure of the use of offsets to achieve net-zero and GHG reduction plans starting January 1, 2025. More widely applicable, AB 1305 also requires website disclosure relating to certain claims regarding the achievement of net zero emissions, "carbon neutral" products and other similar climate claims, as well as other information on progress toward disclosed goals.

Reporting in a Multi-Jurisdiction Environment—Takeaways

In 2025, companies will face multiple new reporting mandates, heightened litigation and related risks and divergent attitudes and views toward disclosure, climate action and ESG initiatives. Companies should consider following key takeaways as they navigate the new environment on climate and ESG rules and risk:

- **Ongoing disclosure requirements: companies still need to prepare for and begin reporting**. Many U.S. and other multinational companies will be subject to CSRD or the CA Climate Rules, regardless of any eventual repeal or invalidation of the Climate Rule. While some of the detailed financial reporting in the Climate Rule will not be required, for many companies climate risk related disclosure and Scope 1, 2 and in some cases, Scope 3, emissions reports, assured by a third-party, will still be required starting in 2026. A main difference is that, at least with respect to CSRD and the CA Climate Rules, U.S. companies will be able to continue to file climate and sustainability information in a separate report and avoid the heightened liability regime of U.S. reporting. However, regardless of the Climate Rule, the general SEC mandate that companies must disclose all material information still applies — including climate change and social matters material to companies' existing business, strategy and goals, and the material financial impacts of company actions and responses to such matters.

- **Companies will increasingly need to manage and watch for competing views on disclosure and litigation around climate and ESG disclosure, and manage internal processes to provide consistent information**. Companies face different sentiments toward the value of climate and ESG reporting from investor groups, regulators and other stakeholders

[10] CARB, "The Climate Corporate Data Accountability Act Enforcement Notice" (December 5, 2024), available here.

Over the next few years, we expect Europe and the U.S. will likely further diverge in approach to climate and other ESG mandates.

around the world. There is increasingly litigation from groups on both sides of the political aisle, some pushing for more disclosure and action and others critical of ESG policies and concerned about related business risks and expenses. Companies should be mindful of risk and liability concerns and keep in mind that any public disclosures may subject them to future regulatory or legal action. In balancing interests and mitigating risk, companies should consider limiting disclosure to those necessary to comply with regulatory requirements and, to a lesser extent, significant investor consensus. For example, while the Nasdaq diversity disclosure rule was vacated, many institutional investors still request information on gender and racial and ethnic characteristics of board members. In response to requests for information from vendors and other stakeholders, including investors, whether in questionnaires or in sustainability reports or SEC filings, companies should maintain a consistent, disciplined approach, including a widely vetted process that includes internal stakeholders from legal, sustainability and investor relations/marketing or communications groups to help ensure appropriate responses in light of legal mandates and liability risk.

- **Companies should continue to monitor other U.S. state and non-U.S. jurisdictions for applicable new disclosure mandates.** Over the next few years, we expect Europe and the U.S. will likely further diverge in approach to climate and other ESG mandates, including increased regulation in Europe (including the CSDDD[11]) with a contrasting deregulatory environment in the U.S. Other jurisdictions may propose more new standards, creating a panoply of disclosure regimes. For example, the 2023 ISSB Standards, voluntary standards intended to create a global baseline to consolidate disclosure frameworks, are being considered for adoption by several jurisdictions outside of Europe. In light of expectations around the Climate Rule, certain state legislatures and executives may expand efforts, similar to the CA Climate Rules,[12] while other states will continue to enact laws or promulgate regulations deemphasizing climate and ESG disclosure and action, including by limiting investment by public entities in certain climate or ESG-related investments. Given the time and resources needed to comply with these differing requirements, companies will need to continue to understand applicable rules and regulatory developments.

[11] For details on the CSDDD, see our March 2022 alert memo available here.

[12] For example, on December 26, 2024, New York enacted a new climate liability law that would require fossil fuel companies to share in payments of $75 billion to address the effects of climate change in the state. The law follows a similar one in Vermont. While the New York law is expected to be challenged, these efforts may pave the way for other states to enact far reaching laws relating to emissions. While the New York law assigns liability based directly on production of fossil fuel, future legislative or regulatory efforts could draw from information provided under existing or new disclosure mandates.

Cybersecurity Disclosure and Enforcement Developments and Predictions

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

Rahul Mukhi
Partner
New York
rmukhi@cgsh.com

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

Nina E. Bell
Capital Markets
Attorney
London
nbell@cgsh.com

Greg Stephens
Associate
Washington, D.C.
gstephens@cgsh.com

The SEC pursued multiple high profile enforcement actions in 2024, alongside issuing additional guidance around compliance with the new cybersecurity disclosure rules. Together these developments demonstrate a continued focus by the SEC on robust disclosure frameworks for cybersecurity incidents. Public companies will need to bear these developments in mind as they continue to grapple with cybersecurity disclosure requirements going into 2025.

SEC Disclosure Rules and Guidance

The SEC's cybersecurity disclosure rules became effective in late 2023, and 2024 marked the first full year of required compliance. The rules added Item 1.05 to Form 8-K,[1] requiring domestic public companies to disclose certain information within four business days of determining that they have experienced a material cybersecurity incident, including the material aspects of the nature, scope and timing of an incident and the material impact or reasonably likely impact of the incident on the company.

The SEC focused considerable effort on providing additional guidance on how it expects companies to comply with the cybersecurity rules. After observing developing practice for six months, the SEC staff published five additional Compliance and Disclosure Interpretations (C&DIs) in June 2024, clarifying certain points with respect to materiality determinations in connection with the rules.

---

[1] The final rules also amended Form 6-K to add "cybersecurity incidents" as a reporting topic for foreign private issuers.

The SEC focused considerable effort on providing additional guidance on how it expects companies to comply with the cybersecurity rules.

Erik Gerding, the outgoing Director of the SEC Division of Corporation Finance, also issued two statements at the time relating to disclosure of cybersecurity incidents. One statement noted, in response to multiple companies filing Item 1.05 Form 8-Ks for incidents for which they had not yet made a materiality determination or that they had determined were not material, that in these circumstances, companies should instead disclose the incident under a different item of Form 8-K (for example, the catchall Item 8.01), to allow investors to more easily distinguish between incidents that have been determined to be material and those that have not.

Finally, the SEC issued comments to several companies that had filed Item 1.05 Form 8-Ks. The majority of these comments were issued to companies that, prior to the June 2024 guidance, had disclosed incidents under Item 1.05 that they had not determined to be material. Companies generally noted that they would consider that guidance going forward.

Enforcement

Cybersecurity incident response and related disclosures remained a priority for agency enforcement throughout the year. Notably, this year's headline actions were brought based on conduct occurring prior to the new Form 8-K requirements taking effect. Additionally, the cases involved either no-admit, no-deny settlements or allegations that have not been tested at trial. For further discussion, *see* An Active Year in Enforcement, with Changes to Come.

Of particular note were a settled enforcement action in June against R.R. Donnelley (RRD), a Manhattan federal judge's July decision granting in part and denying in part SolarWinds's motion to dismiss certain charges relating to a well-known cyber attack in 2020, and more recent enforcement actions and settlements against companies that were victims of cyber attacks. While the SEC suffered a setback in the *SolarWinds* case, actions settled both before and after that decision demonstrated an appetite to aggressively pursue what the SEC perceived to be inadequate disclosure controls or potentially misleading post-incident disclosures.

R.R. Donnelley Settles Inadequate Security Alert Response Allegations

In July of 2024, business communications and marketing services company R.R. Donnelley & Sons Co. agreed to pay $2.1 million to resolve an SEC investigation into alleged deficiencies in RRD's disclosure controls and internal controls, both related to a 2021 cyber attack. The SEC alleged that RRD did not allocate enough resources to manage alert monitoring reports produced by a contracted third party monitoring service and did not adequately instruct the service provider on escalation procedures.

Notably, the SEC was concerned with RRD's failure to maintain cybersecurity procedures and controls designed to escalate relevant aggregated *security alerts*, in addition to *confirmed incidents* to management personnel and disclosure decision-makers in a timely manner. This focus on failure to escalate alerts casts a much wider net for disclosure controls relating to general anti-fraud provisions than incidents that would need to be escalated for consideration of whether disclosure is required under Form 8-K. With this in mind, registrants should analyze their entire incident response process to determine if controls and procedures are in place to not only detect material incidents and potential security events, but also to direct front line reviewers how to appropriately escalate such information and to consider the materiality of incidents in the aggregate.

The SEC also took issue with RRD's capacity for responding to alerts. Highlighting a perceived inability to adequately manage the large volume of escalated alerts, the enforcement order alleged that "the staff

members allocated to the task of reviewing and responding to these escalated alerts had significant other responsibilities, leaving insufficient time to dedicate to the escalated alerts and general threat-hunting in RRD's environment."[2] Registrants should consider whether their internal and external security teams have sufficient time and resources to dedicate to reviewing and potentially escalating alerts. Companies should be prepared to defend the adequacy of those staffing and resourcing decisions based on historical needs.

Registrants should analyze their entire incident response process to determine if controls and procedures are in place to not only detect material incidents and potential security events, but also to direct front line reviewers how to appropriately escalate such information and to consider the materiality of incidents in the aggregate.

Dismissal of Most SEC Claims Related to SolarWinds

SolarWinds Corp. suffered a significant cyber attack dubbed "SUNBURST" that was discovered in December 2020. The attack corrupted the security of SolarWinds' software products, resulting in subsequent security incidents that impacted SolarWinds customers, including the federal government, certain state governments and many Fortune 500 companies. The SEC filed a complaint against SolarWinds and its Chief Information Security Officer in October 2023, alleging they made false statements in violation of the antifraud provisions of the federal securities laws, by touting the strength of their cybersecurity practices in the period before they learned of the SUNBURST incident, and by misleadingly minimizing the extent of the intrusion after it was discovered. The SEC also accused SolarWinds of having such poor cybersecurity and incident reporting procedures that it constituted a violation of the internal controls and disclosure controls provisions of the securities laws.

In July 2024, a judge in the Southern District of New York dismissed the claims relating to the pre-incident media and disclosures, post-incident Form 8-Ks, disclosure controls, and internal controls. The only claim that the district court has permitted to proceed alleges that SolarWinds released a Security Statement that materially misrepresented their internal access controls. The *SolarWinds* decision leads to several important takeaways.

First, the decision strikes a blow against the SEC's contention that cybersecurity controls are part of the system of internal control over financial reporting required by securities laws. The opinion contained persuasive logic that may frustrate an appeal or further attempts at this line of argumentation in future SEC actions. Consequently, the SEC may refocus their efforts towards disclosures and disclosure controls, as they have historically.

Second, the *SolarWinds* case serves as a reminder that companies can be liable in an enforcement action for public statements that are not contained in SEC filings and that may not even be intended for investors. Companies and boards of directors should be aware of what statements are made in marketing materials, security statements, ESG statements, and other public statements that are part of the "total mix of information" available to investors.

Third, courts may distinguish between highly general statements touting a strong cybersecurity posture, which may be dismissed as mere puffery that is not important to investors, and concrete statements about specific cybersecurity practices, which can give rise to a fraud claim if a company is not following those practices with consistency. Here, the order dismissed claims related to generic statements from SolarWinds that it "places a premium on the security of its products" and "makes sure everything is backed by sound security processes" while declining to dismiss claims related

[2] *See* "In the Matter of R.R. Donnelley & Sons Co." (June 18, 2024), available here.

to statements such as SolarWinds's representation that its "password best practices enforce the use of complex passwords that include both alpha and numeric characters."

Fourth, the opinion highlights the importance of providing supplemental disclosures when the victim of a cyberattack determines additional material information about the incident. An additional Form 8-K filed by SolarWinds in January 2021 was cited in the opinion as evidence of the company's lack of fraudulent intent regarding any possible prior material omissions. This point highlights the importance for companies to file follow-up disclosures after a cyberattack, as appropriate, as the SEC highlighted in the Form 8-K requirements.

Settlements With Victims of SolarWinds Attack

In October, the SEC announced settled enforcement actions charging four companies that experienced cyber intrusions due to utilization of infected SolarWinds software. All four companies were involved in IT services and experienced security incidents. The SEC alleged that two of the companies materially misled investors because they used the same generic risk factor disclosures about potential cyber attacks as they did before the breach. The other two companies did provide updated post-breach disclosures, but the SEC alleged these disclosures were misleading by omission, because the companies allegedly downplayed the extent of the intrusions by omitting details that would have been material to investors, such as the fact that the threat actor behind the breach was likely a state actor; the extent of the threat actor's activity in each company's environment; and the amount and importance of the code that was exfiltrated. When considered together with the *SolarWinds* opinion, these actions provide a few takeaways worth considering.

The SEC did not allege that any of the charged companies' cybersecurity practices violated the Exchange Act's internal controls provisions. It is unclear if this absence was due to policy change at the SEC after the *SolarWinds* ruling or merely a reflection of factual differences between by the situations. On the other hand, the SEC did allege failure to maintain proper disclosure controls against one of the companies, asserting that it had no procedures to ensure that, in the event of a known cybersecurity incident, information would be escalated to senior management. Notably, many months elapsed between when the intrusion was discovered by first line security alert reviews and when senior management was alerted.

These actions against victims of cyber-incidents demonstrate the aggressive enforcement posture under Chair Gary Gensler's SEC, despite losses on similar points on the motion to dismiss in the SolarWinds case. A dissenting statement by Republican Commissioners Hester Peirce and Mark Uyeda, who also dissented from the vote to bring the SolarWinds action, shed some light on how things may shift following the upcoming administration change. Calling this action "Monday morning quarterback[ing]," the Republican Commissioners argued that these actions were largely victim blaming, especially when the companies had disclosed the incidents and the SEC was nitpicking the quality of the disclosures. The dissent also argued that the statements or omissions at issue would not actually be material to a reasonable investor. We believe it is unlikely that these sort of cases will be brought under the new administration of Chair-nominee Paul Atkins, with the new administration focusing on violations of the new disclosure rules and actual investor harm.

Finally, the settlements indicate that the SEC will give heightened scrutiny to disclosures by companies in sectors such as information technology and data security, because in their view cybersecurity breaches are more likely to affect these companies' reputation and ability to attract customers.

Flagstar Financial Settlement

The Flagstar Financial, Inc. settlement released on December 16, 2024, provides an indication of the type of cybersecurity case the SEC is more likely to focus on under the next administration.[3] In a no-admit/no-deny settlement in which Flagstar paid a $3.55 million penalty, the SEC alleged that Flagstar negligently made materially misleading statements regarding the late 2021 "Citrix Breach" that resulted in the encryption of data, network disruptions, and the exfiltration of personally identifiable information for approximately 1.5 million individuals. The SEC took issue with 2022 Flagstar filings representing that the company merely experienced unauthorized "access" to its network and customer data when in reality it was aware that the breach disrupted several network systems and exfiltrated sensitive customer data. The SEC also objected to the company repeating generic risk factor disclosures about the potential for experiencing hacks after the company was already aware of the cyber attack. Taken together, the SEC considered these notices to be misleading. Notably, the Republican Commissioners did not dissent from the Order. This case illustrates the type of cases the upcoming administration is more likely to pursue—those where investors or customers may have been harmed and post-incident disclosures are materially misleading both in downplaying incident severity as well as omitting critical facts.

Conclusion

Companies should take care in deciding how and when to disclose cybersecurity incidents and in crafting disclosures about the potential impact of such incidents, including on Form 8-K and risk factor disclosure. Registrants will need to balance the SEC's concern with over-disclosure under Item 1.05 with the risk of enforcement actions should they fail to disclose facts deemed by the SEC to be material. Given the guidance provided by the SEC, we generally expect registrants will err on the side of filing protective Item 8.01 Form 8-Ks for incidents they are concerned could turn out to be material, but before a definitive materiality conclusion has been reached, which has been the general practice following the SEC guidance in June. Registrants that file an 8-K under Item 1.05 without describing any actual or expected quantitative or qualitative material impact should be ready to explain to the SEC staff their materiality analysis and why they filed under Item 1.05 and not Item 8.01.

When preparing their disclosure, registrants should consider factors such as: whether the threat actor is likely affiliated with a nation-state; whether, or the extent to which, the threat actor persisted in the company's environment; and whether the company should disclose not only the number of files or amount of customer data compromised, but also the importance of the files or data and the uses that can be made of them. If the company seeks to quantify the impact of the intrusion, the SEC will likely scrutinize whether the company selectively disclosed quantitative information in a misleading way. Additionally, if the company quantifies the impact of the intrusion but is aware of gaps in its investigation or in the available data that mean the severity of the impact could have been worse, the SEC may consider it misleading not to disclose those facts.

Looking to the future, the recent dissents by the Republican Commissioners indicate a likelihood of agency focus shifting to a less granular concept of materiality in disclosures. We expect the SEC will focus on situations like that in Flagstar, where there is potential for investor harm, rather than dissecting post-incident reports and company processes. That being said, under the last Trump Administration, the SEC brought a number of blockbuster cyber incident disclosure cases against Yahoo and others, which, combined with the new rules, behooves registrants to pay attention to disclosure and related policies and procedures.

[3] *See* SEC Administrative Proceedings, "SEC Charges Flagstar for Misleading Investors About Cyber Breach" (December 16, 2024), available here.

Delaware's Rocky Year – What Lies Ahead?

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

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

Peter Carzis
Associate
New York
pcarzis@cgsh.com

2024 was a remarkable year in Delaware. For the first time in as long as anyone can remember, people began to seriously question whether Delaware would retain its dominance as the go-to jurisdiction for incorporating companies. There was an uproar following several decisions by the Delaware Court of Chancery that seemed to shake the market's confidence in Delaware law's venerable predictability. One such decision invalidated shareholder agreement provisions that had long been commonplace and another found that a board had not validly approved a merger agreement because, as is typical, the board had not received a draft in final form. At the same time, a certain well-known CEO's $50 billion compensation package was struck down, leading him to publicly declare "Never incorporate your company in the state of Delaware."[1]

In the face of this public pressure, the Delaware legislature moved at unprecedented speed to amend the Delaware General Corporation Law (DGCL) in order to "overrule" several of the decisions that caused the most immediate concern (to the consternation of many, including the judges who had decided the cases that were overruled). But a sense of unease persists, especially regarding the Delaware courts' recent perceived hostility towards controlling stockholders. For this reason, several controlled companies have already elected to leave Delaware for other jurisdictions such as Nevada or Texas—in one such case, the

[1] *See* this post from Elon Musk on X (January 30, 2024), available here.

Delaware Court of Chancery found the decision to leave should be reviewed under the entire fairness test, although the Delaware Supreme Court quickly accepted an interlocutory appeal (which remains pending) to reconsider that issue.

In the face of this public pressure, the Delaware legislature moved at unprecedented speed to amend the Delaware General Corporation Law in order to "overrule" several of the decisions that caused the most immediate concern.

Still, notwithstanding the turbulence in Delaware, there has been no mass "DExit."[2] In large part, that is because it remains unclear whether other jurisdictions would "solve" the perceived problems Delaware is facing. Nevada and Texas, among others, have publicly sought to lure companies away from Delaware, including by setting up dedicated business courts intended to operate like the Delaware Court of Chancery and pointing to differences in their corporate statutes. But it remains to be seen how these courts will operate in practice, and numerous questions abound as to how these states' corporate laws will be applied in the seemingly countless circumstances that have been addressed by Delaware's statutory and decisional law over many decades. Meanwhile, notwithstanding the grumbling, Delaware courts remain unparalleled in their sophistication on corporate issues and in their ability to decide complex cases expeditiously.

Below we summarize some of the key developments in Delaware law over the past year and give a preview of what we think is coming in 2025.

[2] *See* Stephen Bainbridge "DExit Drivers: Is Delaware's Dominance Threatened?" (September 6, 2024), available here.

Moelis, Activision, Crispo and the 2024 DCGL Amendments

Much of the controversy and uncertainty that characterized Delaware's acrimonious 2024 stemmed from three decisions in particular that many believed upset the status quo on key points of corporate law, and which, in turn, were legislatively overruled by Delaware lawmakers. The decision that garnered the most attention was *West Palm Beach Firefighters' Pension Fund v. Moelis & Co*,[3] in which the Court of Chancery held that stockholder agreement provisions imposing a pre-approval requirement on certain board actions, which are common, were facially invalid under the DGCL.[4] Following the decision's announcement, many observers noted an apparent misalignment between this outcome and conventional assumptions about the validity of such provisions—even the court tacitly conceded as much, chiding: "[w]hen market practice meets a statute, the statute prevails."[5] In response, the summer 2024 amendments to the DGCL added a new provision aimed at restoring the validity of that "market practice" by expressly permitting provisions that restrict or prohibit the corporation from taking specific actions.[6]

The legislative amendments also addressed the Court of Chancery's February 2024 decision in *Sjunde AP-fonden v. Activision Blizzard, Inc*.[7] In *Activision*, the court held that the Defendant's board had approved an insufficiently complete merger agreement, again as is common practice.[8] Here too the court eschewed alignment with market practice—warning that "[w]here market practice exceeds the generous bounds of private ordering afforded by the DGCL, then market practice needs to check itself"[9]—and again, Delaware lawmakers responded with a return to what many believed had been the status quo: the DGCL was amended so as to

[3] 311 A.3d 809 (Del. Ch. 2024).

[4] *Id. at 870.*

[5] *Id. at 881.*

[6] DGCL § 122(18).

[7] No. 2022-1001-KSJM, 2024 WL 863290 (Del. Ch. February 29, 2024), *as corrected* (March 19, 2024).

[8] *Id.* at *8-10.

[9] *Id.* at *6.

pare back the specific requirements for "essentially complete" merger agreements for purposes of board approval.[10]

Finally, the DGCL amendments likewise overruled the Court of Chancery's decision in *Crispo v. Musk*,[11] in which the court had held that a merger agreement's lost-premium provision (giving the target company the right to seek lost premium damages against the buyer on behalf of its stockholders) was not enforceable either by the target company's stockholders or by the company itself.[12] In response to the perceived problems created by this decision (including that buyers may be able to walk away from a deal without having to pay the full costs of doing so), Delaware lawmakers amended the DGCL to permit parties to a merger agreement to allow the target company to sue the buyer for damages equal to "the loss of any premium or other economic entitlement" that the target stockholders would have received if the deal were consummated.[13]

Judicial Scrutiny Of "Conflicted Controller" Transactions

2024 saw also a year in which the Delaware Courts directed increased skepticism toward controlling stockholders whose interests they perceived as in conflict with those of the corporation, including by increasing the scrutiny with which the fairness of conflicted-controller transactions is assessed. In *In re Match.com Derivative Litigation*,[14] for example, the Delaware Supreme Court expressly declined to review conflicted controller transactions outside of the "squeeze out" context under the Business Judgment Rule if they were approved by an independent committee of directors. Instead, the Supreme Court held that the only way for defendants to shift the standard of review for such transactions from Entire Fairness to the Business Judgment Rule, as in the squeeze out context, is to comply with the full "MFW" framework (*i.e.*, the controlling stockholder commits "ab initio" to subject the transaction to the approval of both (a) an independent committee and (b) a majority of the minority stockholders).[15]

The Court of Chancery also arguably expanded what constitutes a "conflict" (or "non-ratable benefit" received by the controlling stockholder) in *Palkon v. Maffei*.[16] This decision concerned TripAdvisor's decision to leave Delaware and reincorporate in Nevada, an action motivated in part (as acknowledged in the proxy statement) by the controlling stockholder's and directors' desire for the greater legal protection afforded fiduciaries in Nevada.[17] The *Palkon* Court held that the decision to relocate in this case was subject to the Entire Fairness standard since the transaction conferred a non-ratable benefit upon the Company's controller and other corporate fiduciaries, even though there was no threatened litigation at the time.[18] The Delaware Supreme Court, however, accepted an interlocutory appeal from this decision; that appeal remains pending.

The Court of Chancery's decision in *In re Sears Hometown and Outlet Stores, Inc. Stockholder Litigation* further expanded the responsibilities and challenges controllers face by holding that they may owe fiduciary duties to other stockholders even when they act purely as stockholders.[19] This dispute emerged when the corporation's majority shareholder disagreed with certain board members over a proposed liquidation plan that the controller believed would destroy value; ultimately, the controller prevented the plan from coming to fruition by taking action as a stockholder to remove two directors, and amend the bylaws to require that certain board actions be approved by at least 90% of the directors in two separate votes taken at least thirty business days apart.[20] Minority stockholders then

10 DGCL § 268.

11 304 A.3d 567 (Del. Ch. 2023).

12 *Id.* at 584-85.

13 DGCL § 261(a)(1).

14 315 A.3d 446 (Del. 2024).

15 *Id.* at 462-63.

16 311 A.3d 255 (Del. Ch. 2024), *cert. denied*, No. 2023-0449-JTL, 2024 WL 1211688 (Del. Ch. March 21, 2024)

17 *Id.* at 263-64.

18 *Palkon*, 311 A.3d, 283-84 (Del. Ch. 2024).

19 309 A.3d 474 (Del. Ch.), *modified on reargument*, (Del. Ch. 2024).

20 *Id.* at 492-504.

claimed that the controller had breached his fiduciary duties as a controlling stockholder by taking such action. Even though it has been traditionally understood that stockholders—even controlling stockholders—owe no fiduciary duties when exercising their stockholder-level powers (such as the right to vote their shares), the court held that "when exercising voting power affirmatively to change the status quo, a controlling stockholder owes a fiduciary duty of loyalty which requires that the controller not intentionally harm the corporation or its minority stockholders, plus a fiduciary duty of care."[21] The court thus reviewed the controller's removal of directors and changes to the bylaws under enhanced scrutiny. The court ultimately held that the controller's actions were not done in breach of his fiduciary duties because the controller demonstrated that he acted properly and good faith to prevent the destruction of value that he believed the liquidation would cause.[22]

Finally, this expansion of a controlling stockholder's duties was coupled with a parallel expansion of what it means to *be* a controlling stockholder in the first place. In *Tornetta v. Musk*, a dispute over the Tesla's CEO's compensation, the Court of Chancery emphasized that a "mathematical majority of the corporation's voting power" represents only one of a number of "indicia of control."[23] Arriving at a multifactorial analysis that "call[s] for a holistic evaluation of sources of influence," the court weighed pure voting power alongside additional criteria including "the right to designate directors," "decisional rules in governing documents that enhance the power of a minority stockholder or board-level position," and "the ability to exercise outsized influence in the board room, such as through high-status roles like CEO, Chairman, or founder."[24] As a result, the Chancery Court held that Musk was a controlling stockholder of Tesla despite holding only 21.9% of voting power, suggesting that a more capacious conception of the conflicted controller transaction may be ascendant in Delaware courts.[25]

Plaintiff Lawyer-Driven Attacks on Common Bylaw Provisions

Finally, 2024 also saw Delaware courts invalidate a number of provisions common among advance notice bylaws in *Kellner v. AIM Immunotech Inc.*, leading to attempts by plaintiffs' firms to challenge these and other bylaw or charter provisions in hopes of collecting fees.[26] The *Kellner* case stemmed from a longstanding proxy contest between AIM's board and certain activist stockholders; amidst this proxy contest, AIM amended its bylaws to add "advance notice" provisions that are common among public companies and designed to ensure stockholders are fully informed about any insurgent-backed slate.[27] Relying on these amendments, the board then rejected the alternate slate's nomination on the basis that the notice submitted in connection with their candidacy was deficient, and the stockholders challenged the amended provisions' validity.[28]

The Court of Chancery declared a number of these provisions invalid, finding that they stood to "inequitably imperil the stockholder franchise to no legitimate end."[29] These included provisions requiring that the nominating stockholder disclose all arrangements, agreements or understandings (AAUs), which was expansively defined, among others.[30] Ultimately, however, the court found the board's rejection of the nomination to be valid due to the Plaintiffs' breach of certain other provisions that the court found to be enforceable.

21 *Id.* at 516.

22 *Id.* at 518, 537-39.

23 *Id.* at 500.

24 *Id.* (quoting *Basho Techs. Holdco B, LLC v. Georgetown Basho Invs.*, LLC, No. CV 11802-VCL, 2018 WL 3326693 at *27 (Del. Ch. July 6, 2018), *aff'd sub nom. Davenport v. Basho Techs. Holdco B, LLC*, 221 A.3d 100 (Del. 2019)).

25 *Id.* at 500-02.

26 320 A.3d 239 (Del. 2024).

27 *Id.* at 246-51.

28 *Id.* at 251-52.

29 *Kellner v. AIM ImmunoTech Inc.*, 307 A.3d 998, 1006 (Del. Ch. 2023), *judgment entered*, (Del. Ch. 2024), *and aff'd in part, rev'd in part*, 320 A.3d 239 (Del. 2024).

30 *Id.* at 1027-35.

The *Kellner* decision provides important guidance for boards as they plan on a "clear day" for a potential proxy contest in the future.

On appeal, Delaware Supreme Court clarified that when bylaw provisions are facially challenged (*i.e.*, in the absence of a live proxy contest or similar dispute), the bylaws should be upheld if there is any circumstance in which they could be enforceable.[31] However, given the live proxy contest in this case, the Supreme Court applied enhanced scrutiny to the provisions at issue and agreed with the Court of Chancery that they were unenforceable, albeit only on an as-applied basis.[32]

While the Supreme Court's *Kellner* decision gives companies a powerful defense when stockholders assert facial challenges to their bylaw provisions, that has not stopped plaintiffs' firms from making such challenges, often in the form of "demand letters," and sometimes escalating into lawsuits.[33] Regardless of the focus of plaintiffs' firms, the *Kellner* decision provides important guidance for boards as they plan on a "clear day" for a potential proxy contest in the future.

Key Takeaways

- We expect the debate over the direction of Delaware corporate law to continue. Notwithstanding the enactment of the DGCL amendments in summer 2024, the controversy surrounding them and other issues has continued to spark lively discussions that go to the core of Delaware corporate law. Should Delaware provide corporate entities and their constituents—stockholders, boards, management, etc.—greater contractual freedom to order their affairs and enter into transactions as they see fit? Or should Delaware courts be more ready to intervene to ensure compliance with statutory and fiduciary duties and the fairness of transactions to minority or disinterested stockholders? While Delaware has historically sought to balance these priorities, they are undeniably in tension with each other. How to balance them will continue to be subject to the push-and-pull dynamic of evolving caselaw and a vigorous debate.

- At the same time, boards should pay attention to developments in Nevada, Texas and other states that seek to challenge the dominance of Delaware in the corporate law realm. As noted above, there are many unanswered questions as to how those states will deal with the corporate law issues that will inevitably arise. Over time, as more companies are incorporated in those states, some of those questions may be answered.

- Meanwhile, in Delaware, we expect in the near-term that transactions involving a controlling stockholder (or stockholder with arguably controlling influence) whose interests are in conflict (or arguably do not align) with the remaining stockholders will continue to attract the attention of the plaintiffs' bar. While the Delaware Supreme Court declined to provide a practical method of cleansing such transactions in the *Match.com* case, it remains to be seen whether the Delaware courts will nonetheless pare back such cases, for example by narrowing the type of "non-ratable benefits" that trigger entire fairness or tightening the standard for finding a stockholder to have control.

- We also expect continued focus by the plaintiffs' bar on commonplace bylaw provisions that are perceived to be in tension with the DGCL or otherwise subject to challenge. While the Delaware Supreme Court cut back on the circumstances in which stockholders can successfully challenge such provisions in the absence of a live dispute, boards may want to consider whether any amendments are desirable in advance of a potential dispute.

[31] *Id.* at 258-63.

[32] *Id.* at 263-66.

[33] *See* Leslie Pappas, "Resignation Letter Bylaws Targeted In Five Del. Class Actions" (May 23, 2024), available here.

The Current Tax Risk Environment and Best Practices for Managing It

Jens Hafemann
Partner
Frankfurt
jhafemann@cgsh.com

Maureen E. Linch
Partner
Bay Area
mlinch@cgsh.com

Richard Sultman
Partner
London
rsultman@cgsh.com

Benjamin Boisanté
Senior Attorney
Paris
bboisante@cgsh.com

Gianluca Russo
Senior Attorney
Milan
grusso@cgsh.com

Peter North
Associate
London
pnorth@cgsh.com

2025 begins with a continuation of the major tax trends emerging in the post-COVID era: more aggressive audits by tax authorities in search of additional revenue, increased international cooperation between tax authorities, the end of transitional concessions to assist businesses through the pandemic, and a developing role for tax in shaping ESG policies and behaviors.

These trends have emerged in an increasingly complex technical tax environment characterized by an accumulation of new rules and the layering of international tax regimes (such as the OECD's global minimum taxation rules) on top of domestic tax regimes. At the same time, regulators are demanding enhanced transparency, tax authorities are mining data with smarter and faster AI tools and governments are getting more efficient at sharing information across borders. Against this background, the management of modern tax risks has become a cornerstone of sound corporate responsibility.

Set out below we have identified some key topical areas of tax risk that multinational groups are commonly encountering, and some best practices for addressing them.

Internal Tax Risk Management: Tax Strategies and Policies

Establishing and maintaining robust internal procedures for identifying, comprehending and mitigating tax risks can lower compliance costs in the long term while allowing more nimble decision making and facilitating a positive relationship with taxing authorities. An effective framework requires involvement and collaboration at every level of an organization, from the board, to senior management, to the audit and risk committees, to the members of each department.

> Trends have emerged in an increasingly complex technical tax environment characterized by an accumulation of new rules and the layering of international tax regimes (such as the OECD's global minimum taxation rules) on top of domestic tax regimes.

Best practices include a clear and documented tax risk management strategy set by the board and audit committee, accountability protocols adopted by the tax, finance, human resources and legal departments, and ongoing review and monitoring by business, accounting and tax teams. Members of the tax and accounting teams should be in regular communication with each other and with business teams and should review all business decisions above a certain materiality threshold. Tax risks should be addressed in a consistent manner as other business risks. Achieving an effective system requires top-down engagement and transparency throughout.

The adoption of a formal (and public) tax strategy is a legal requirement for large companies in some countries. The UK, for example, requires large groups with UK members to publish an annual online strategy document covering the group's attitude to UK tax planning, the level of UK tax risk the business is prepared to accept and how the business works with the UK tax authorities. Large corporate groups might consider something similar even if not formally required.

Tax Authority Risk Management: Cooperative Compliance

Cooperative compliance initiatives are being increasingly adopted by tax authorities around Europe. Originally these initiatives were available only to large companies, but many countries are now considering reducing the relevant thresholds (which are generally based on annual turnover), to expand their reach to mid-sized companies as well as to high-net-worth individuals.

The main goal of a cooperative compliance approach is to ensure tax compliance through an enhanced relationship with the taxpayer. The benefits to the taxpayer—in the form of reduced risk of tax authority challenge and assessments—can be material. Eligible taxpayers who have a history of compliance, who commit to exchange information with the tax authorities on an ongoing basis and who implement other controls to measure, manage and control tax risks can generally expect favorable administrative procedures, such as expedited access to tax authorities as well as enhanced engagement from tax authorities in formal and informal discussions on uncertain tax issues. Timely and comprehensive disclosures under a cooperation agreement can also result in reduced penalties if assessments nonetheless occur.

Organizational Tax Risk Management: Risks Of Modern Working Practices

The post-pandemic shift to mobile and remote working practices has exposed organizations to increased risks of establishing an unintended taxable presence in countries or states where they did not previously report or file returns. This can trigger unplanned corporate income taxes, sales taxes and value added taxes, as well as payroll reporting and withholding obligations. Tax authorities are becoming less accommodating on these matters.

From a corporate income tax perspective, companies generally become subject to tax and filing obligations in jurisdictions where they are considered to be tax resident or in which they are considered to maintain a permanent establishment (PE). Tax residence can often arise in a jurisdiction if management functions are exercised there—some jurisdictions look to the location of board level management and control, whereas others look more at the place of effective day to day management. A PE can arise (even if tax residence does not) if a company has a fixed place of business in a jurisdiction or if it has a dependent agent doing business there on its behalf. Tax residence typically entitles the jurisdiction of residence to impose taxation on the company's worldwide profits, whereas the presence of a PE generally entitles the relevant jurisdiction to impose tax on profits of the company attributable to the PE. Similar considerations are also relevant for other taxes (such as VAT and other trade taxes).

Regulators are demanding enhanced transparency, tax authorities are mining data with smarter and faster AI tools and governments are getting more efficient at sharing information across borders.

Many tax authorities relaxed their enforcement of rules for determining tax residence or the existence of PEs during the pandemic. However, under renewed pressure to increase tax revenues, and with the benefit of recent extensions to international treaty-based rules for when PEs are deemed to exist, those authorities are clamping back down. Consequences can be severe—in some European jurisdictions, for example, an undisclosed PE can result in significant penalties and potential criminal exposures.

Considering these risks, groups with internationally mobile directors, senior management and other employees, or personnel who work remotely in a different jurisdiction to their employing company, should ensure they have an accurate picture of the applicable rules that apply wherever the relevant individuals regularly perform their duties. Any remote working policies put in place during the pandemic should be revisited with additional safeguards being put in place, where necessary. The same is true for permissions that may have been given for directors to attend board meetings by telephone or video conference. Care should be taken to monitor who does what and from where, with contemporaneous evidence—like board meeting minutes, time sheets and travel records being obtained and retained. In some cases, it may be advisable to prohibit remote working practices or locations in the absence of a clear benefit to the business; in other cases it may make sense to embrace a taxable presence in a new place and to set up a local entity to house relevant individuals. Targeted solutions may be available for certain risks, like engaging local professional employer organizations (PEOs) to take on the legal, tax and compliance burdens associated with payroll obligations for remote workers.

Transactional Tax Risk Management: The Use Of Insurance Policies

Transactional tax risks are traditionally managed either through contractual arrangements that allocate the risks between the parties (for example in the tax warranties or tax indemnity provisions of a share purchase agreement) or, if available, advance tax rulings issued by the competent tax authority. However, both approaches have limitations:

- Trying to manage tax risks through contractual arrangements remains subject to negotiation power and ultimately counterparty/solvency risk. Also, classic tax indemnities do not typically provide for a "clean break." Due to customary international tax audit cycles, tax risks often take some years to surface, so parties to a tax indemnity will often only know years after a transaction has closed whether a tax risk could materialize, and they could then remain entangled with each other for subsequent years based on applicable statutes of limitations and tax assessment and appeal processes.

- Tax rulings, if available, often take too long to be obtained to be a practical tool to address risks arising on deals. They also can trigger significant statutory administrative fees and/or the materialization of tax risks. Furthermore, tax rulings are in many jurisdictions limited to future, yet unimplemented fact patterns and so are not able to address scenarios relating to past transactions.

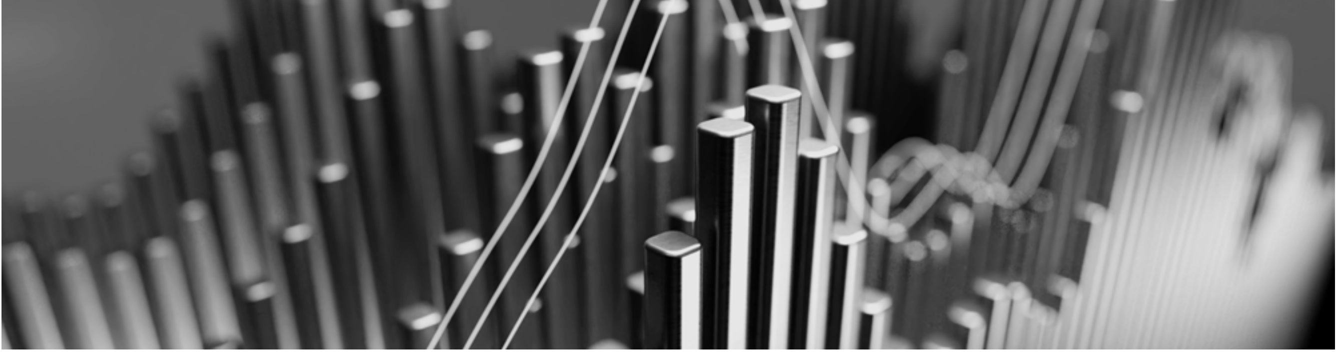
Many varieties of tax insurance policies have been (and are continuing to be) developed to provide solutions to these concerns:

- Warranty and indemnity (W&I) insurance policies regularly cover tax risks that have not been identified in tax due diligence. Typically, the buyer is required to take out a W&I policy, and the seller's liability under the purchase agreement is either excluded or limited to a symbolic one Euro/Dollar—all subject to satisfactory customary tax due diligence and customary exclusions (such as transfer pricing and fraud). In such cases, the W&I policy covers liability scenarios in which the seller would otherwise be liable under the purchase agreement's tax warranty and indemnity provisions.

- An evolving trend in tax W&I policies is for cover to not strictly be linked to the provisions of the purchase agreement: so-called synthetic/virtual insurance policies are, if available, able to cover fact patterns that are not covered under the indemnity provisions in a typical purchase agreement, including extending the statute of limitations beyond the survival provisions or "scraping" knowledge qualifiers in warranties.

- Tax insurance policies may also be available in relation to certain known tax risks identified in tax due diligence. This so-called special tax liability insurance is often promoted on the basis that it is obtainable faster than a tax ruling, it can cover known but not yet materialized tax risks resulting from past events, and it can bridge risk allocation gaps between the seller and the buyer.

Although tax insurance coverage can often provide solutions on M&A transactions, it can come with drawbacks too. Obtaining the insurance adds another work stream that will require a certain level of tax due diligence, the negotiation of the insurance policy and additional fees, premiums and potentially insurance premium taxes. Other than for the most standard W&I policy (and certainly not in the case of a special tax liability policy) insurance is not a one-size fits all solution and will require tailoring to each deal. In some cases, the timing and cost required to put insurance in place, or the exclusions and other burdensome terms of the policy may outweigh accepting the risk.



2025 UK and European Capital Markets Update: "All Change!"

UK and European capital markets underwent significant reform in 2024. The UK Financial Conduct Authority (FCA) overhauled the UK listing regime and implemented new listing rules (UKLRs) as part of the UK government's efforts to simplify and modernise the regime and reinvigorate the UK capital markets. The UKLRs pave the way for further reform of the UK's prospectus and public offer regimes, with final rules expected in the summer. In the EU, the EU Listing Act introduces fundamental changes—to the EU market abuse and prospectus regimes, in particular—which are intended to simplify and standardise requirements for EU listed issuers. The EU Listing Act is part of the EU's Capital Markets Union project aimed at increasing the attractiveness of EU capital markets. These reforms have generally been positively received on both sides of the Channel. Despite some alignment amongst the reforms (whether implemented or proposed), they also introduce notable divergence between the UK and EU regimes, for the first time since Brexit.

Chrishan Raja
Partner
London
craja@cgsh.com

Alexandre H. Pauwels
Associate
London
apauwels@cgsh.com

Annie Cowell
Associate
London
acowell@cgsh.com

Bree Morgan-Davies
Practice Development
Lawyer, London
bmorgan-davies@cgsh.com

Alexander Lees
Trainee Solicitor
London
alees@cgsh.com

Reform of the UK Listing Rules

Overview

July 29, 2024 marked a fundamental change to the UK listing regime, as the FCA's landmark reforms to the UKLRs came into effect. At the core of the UKLR reforms is the replacement of the standard and premium listing categories of the FCA's Official List with a single listing category for shares in commercial companies, and a more streamlined set of rules relating to eligibility and continuing obligations. Companies looking at primary listings, especially companies with no or limited operating history, as well as companies with a complex financial history, which may have been discouraged from listing before, may want to consider UK listings in light of the reforms.

Context for Reform

In response to a significant decline in UK listings (and initial public offerings globally),[1] the "UK Listings Review" was launched by the UK government in November 2020 to consider and improve the UK's position as a global financial centre. Building on the recommendations of that Review, the FCA has been consulting on a series of reforms to simplify and modernise the UK listing regime, including the new UKLRs and other proposed revisions to the UK's prospectus and public offer regimes.

Cohesively, these reforms will look to shift greater discretion and responsibility to the FCA, lower regulatory barriers and ease the capital-raising process for companies seeking to list in London, while maintaining the high standards of corporate governance, shareholder rights and transparency associated with a London listing. Following the implementation of the ULKRs, further reform is expected including a new prospectus regime which will revoke and replace the current UK Prospectus Regulation.[2] We focus here on the impact of the new UKLRs.

---

[1] Per the FCA "Primary Markets Effectiveness Review: Feedback to CP23/10 and detailed proposals for listing rules reforms" (December 2023) available here and the UK Listing Review, there has been a 40% decline in the number of companies listed in the UK between 2008 and 2020, noting that the UK accounted for only 5% of global initial public offerings of companies between 2015 and 2020.

[2] In January 2024, HM Treasury published "Public Offers and Admissions to Trading Regulations 2024 (SI 2024/105) (POAT Regulations)" available here, establishing the framework for a new UK prospectus regime. In July 2024, the FCA published "Consultation on the new Public Offers and Admissions to Trading Regulations regime (POATRs)" available here on the new prospectus regime, including rules set out in a new "Prospectus Rules: Admission to Trading on a Regulated Market" sourcebook which will replace the existing Prospectus Regulation Rules. The FCA aims to finalise the rules by the end of H1 2025.

Notable Updates

- **Single listing category**. The FCA has departed from its historic dual structure of premium and standard listings, replacing them with a single listing category and set of rules for "equity shares in commercial companies" (ESCC).[3] Listing categories for other types of instrument and issuer are also in effect, including a new "transition" category for issuers that had an existing listing on the date the new UKLRs came into force. In keeping with the FCA's stated aim to encourage a diverse range of companies to list and grow on UK markets, there is no definition of what constitutes a "commercial company," and admission to the ESCC category is not restricted to issuers with specific business models.

- **Eligibility requirements**. The new UKLRs retain the core set of eligibility requirements that applied to all equity share listings under the previous regime (such as the 10% minimum free float and market capitalization requirements). However, financial eligibility criteria once applicable to premium listings has been dropped, notably the requirements to produce i) a three-year revenue earning track record; and ii) an unqualified working capital statement. These changes will allow companies with no or limited operating history, as well as companies with a complex financial history, to list on the ESCC listing category. The current UK Prospectus Regulation continues to require a working capital statement (although this may be qualified). The FCA's broad powers to assess eligibility for listing, and to refuse applications where it considers listing would be detrimental to the interests of investors, remain.

- **Significant transactions regime**. Prior to reform, shareholder approval and publication of an FCA-approved disclosure document were required where a proposed transaction was 'significant' as determined by the class tests, which assess the size of a transaction by reference to certain percentage ratios. Under the new UKLRs, shareholder approval of "significant" transactions (*i.e.*, transactions meeting the 25% threshold, based on retained class tests) is no longer required, but disclosure must be made to the market (though no FCA approval of the disclosure is required). The new UKLR regime provides for: (i) an initial notification with information on the transaction; (ii) follow-on disclosures to be made as soon as the necessary information is available; and (iii) a completion notification. Historical financial information and fairness statements will not be required in the case of acquisitions. The provision for separate notifications affords issuers greater flexibility around the timing and content of announcements for significant transactions.

Companies looking at primary listings, especially companies with no or limited operating history, as well as companies with a complex financial history, which may have been discouraged from listing before, may want to consider UK listings in light of the reforms.

- **Related party transactions**. Prior to reform, shareholder approval and publication of an FCA-approved disclosure document were required for certain transactions between a listed company and its related parties (assessed, based on the size of the transaction). Under the new UKLRs, related party transactions will no longer require shareholder approval. The FCA has instead endorsed a disclosure-based approach (though no FCA approval of the disclosure is required), enhanced by additional governance requirements. The previous disclosure requirements for smaller related party transactions, where percentage ratios fall between 0.25% and 5%, have been removed in their entirety. Any such transactions at or above the 5% threshold will require board approval (excluding any conflicted directors) and a timely market announcement including a "fair and reasonable" statement from

[3] Cleary Gottlieb recently advised on Canal+ S.A.'s listing on the London Stock Exchange, one of the first listings within the *Equity Shares—commercial companies* listing category.

the board of directors, with written support from a sponsor (see below for further information on sponsor requirements). Further, a party now becomes a "substantial shareholder", and thus a related party, at 20% of voting rights in the company, as opposed to 10% prior to the UKLR reforms.

- **Dual class share structures**. Prior to reform, weighted voting rights for main market listed companies could only be exercised in certain limited circumstances. They were permitted to subsist for five years and could only be held by a director. The final UKLRs permit institutional investors or shareholders at the point of listing to hold enhanced voting rights in commercial companies, though there is a 10-year "sunset" (*i.e.*, maximum time restriction) on the exercise of these enhanced voting rights. As such, specified weighted voting rights shares may now be held at the point of listing by: (i) directors; (ii) existing investors or shareholders (natural persons and institutions); (iii) employees; or (iv) persons established for the sole benefit of, or solely owned and controlled by, a person in (i), (ii) or (iii). Holders of specified weighted voting rights shares will not be able to vote in situations where the UKLRs require a shareholder vote to be taken, save for reverse takeovers and the election of independent directors.

- **Controlling shareholders**. An applicant for premium listing was previously required to demonstrate that it intended to carry on an independent business as its main activity. These requirements are abolished for commercial companies, except where a company has a controlling shareholder (broadly, a person who controls 30% or more of the votes). The new UKLRs also remove the requirement for a relationship agreement with a controlling shareholder, although independence will still need to be demonstrated (it remains to be seen how practice evolves on this point). The UKLRs also include a shorter list of factors which may indicate that an issuer is not independent of a controlling shareholder. A further continuing obligation has been included in the UKLRs where a controlling shareholder (or its associate) proposes a resolution that a director considers is intended, or appears to be intended, to circumvent the proper application of the UKLRs. In this case, the circular accompanying such proposal must include a statement of the director's opinion regarding that resolution.

Sponsor Regime

The rules governing sponsors and their conduct of sponsor services remain substantively similar to the previous requirements for a premium listing. FCA reforms have retained the requirements for admission and post-IPO, but have significantly reduced the sponsor's involvement post-IPO to focus on targeted issuer events, including:

- transactions involving additional equity issuances and that require a prospectus;
- reverse takeovers;
- large related party transactions;
- transfers in and out of the ESCC category;
- where an issuer requests individual guidance from the FCA; and
- where an issuer seeks a modification or waiver from the UKLR from the FCA.

Indexation

FTSE Russell announced changes to its Ground Rules in light of the UKLR reforms in November 2024,[4] confirming that companies listed on the ESCC and new closed-ended investment fund categories would be the new index universe for the FTSE UK Index Series, replacing the premium segment.[5] Companies previously admitted to the standard segment would continue to be ineligible for the FTSE UK Index Series under the new

[4] FTSE Russell "FTSE Global Equity Index Series Ground Rules" (November 2024), available here.

[5] For more information on the FTSE changes to the UK Indexation Rules, see our March alert memo available here.

regime. FTSE Russell has not introduced any additional eligibility requirements to replicate previous premium listing requirements.

Transitional Provisions and Next Steps

On July 29, 2024, issuers listed on the premium and standard listing segments were mapped automatically to the relevant new listing categories, subject to the application of certain transitional provisions for "in-flight" applications. Existing premium listed issuers were automatically mapped to the new ESCC category. Existing standard listed commercial companies were automatically mapped to the new "transition" category, which replicates the previous standard listing continuing obligations and is closed to new entrants. Such issuers now have the option to transfer to the ESCC category subject to meeting applicable eligibility requirements, however, the transition category has no fixed end date, so there will be no deadline for issuers to transfer out.

The final UKLRs represent an extensive overhaul of the UK listing regime.[6] The FCA intends to formally review the new listing regime in five years' time to assess its impact on the market but has indicated its willingness to intervene earlier if necessary to ensure market integrity.

[6] For additional information, see our December 2023 alert memo available here and our July 2024 alert memo available here.

Chrishan Raja
Partner
London
craja@cgsh.com

Marijke Spooren
Partner
Brussels
mspooren@cgsh.com

Laurent Legein
Partner
Brussels
llegein@cgsh.com

Alexandre H. Pauwels
Associate
London
apauwels@cgsh.com

Jean-Sébastien Rombouts
Associate
Brussels
jrombouts@cgsh.com

Michiel De Wolf
Associate
Brussels
mdewolf@cgsh.com

Ruben Foriers
Associate
Brussels
rforiers@cgsh.com

Bree Morgan-Davies
Practice Development Lawyer, London
bmorgan-davies@cgsh.com

The EU Listing Act: Important Changes to the EU Market Abuse Regulation and the EU Prospectus Regulation

Regulation (EU) 2024/2809 of the European Parliament and Council of October 23, 2024 (the EU Listing Act)[7] makes important changes to the EU Market Abuse Regulation (EU MAR) and EU Prospectus Regulation (EU PR) that are aimed at alleviating some of the compliance burden for issuers, enhancing legal clarity, addressing disproportionate requirements for issuers and, importantly, increasing the overall attractiveness of EU capital markets, among other amendments.[8] The EU Listing Act entered into force on December 4, 2024.[9] These changes will have a significant impact — which we view as mostly positive — on the compliance practices of issuers listed in the EU.

The most important changes to EU MAR and EU PR are summarized below, along with a brief discussion of the potential impact of these changes for UK issuers.

Entry Into Force

Generally speaking, as an EU regulation, the EU Listing Act is directly applicable in all EU Member States; however, certain changes will apply on a staggered basis depending on their nature. In particular, some changes to EU MAR and EU PR will only become effective after 15 or 18 months.

[7] Regulation (EU) 2024/2809 of the European Parliament and of the Council of October 23, 2024 amending Regulations (EU) 2017/1129, (EU) No 596/2014 and (EU) No 600/2014 to make public capital markets in the Union more attractive for companies and to facilitate access to capital for small and medium-sized enterprises, available here.

[8] For additional information, see our prior memorandums published in October, available here and November, available here.

[9] The EU Listing Act package includes (i) a Regulation amending the Prospectus Regulation (Regulation (EU) 2017/1129), the Market Abuse Regulation (Regulation (EU) No 596/2014), the Markets in Financial Instruments Regulation (Regulation (EU) No 600/2014), (ii) a Directive amending the MiFID II Directive (Directive 2014/65/EU) and repealing the Listing Directive (Directive 2001/34/EC), and (iii) a Directive on multiple-vote share structures in companies that seek the admission to trading of their shares on a multilateral trading facility.

Tom Vanderhaegen
Practice Development Lawyer
Brussels
tvanderhaegen@cgsh.com

Alexander Lees
Trainee Solicitor
London
alees@cgsh.com

A Brief Introduction To EU MAR

EU MAR was introduced in 2016 and establishes a robust framework to preserve market integrity and investor confidence with numerous rules aiming to prevent insider dealing, unlawful disclosure of inside information and market manipulation in the EU. In particular, EU MAR subjects issuers to extensive obligations, including as to disclosure and record-keeping, which have a direct impact on the daily operations of listed companies.

Generally, EU MAR has a broad scope of application, and applies to financial instruments admitted to trading, or for which a request for admission has been made, on an EU regulated market, multilateral trading facility or organized trading facility.[10] "Financial instruments" are defined broadly and include any transferable securities (whether equity or debt), money-market instruments, certain derivatives (including (amongst others) security, currency or interest rate derivatives whether settled physically or in cash, and (optional) cash-settled commodity derivatives), and emission allowances.

Key Changes To EU MAR

*A. **Disclosure of intermediate steps in protracted processes no longer required*** *(Effective: June 5, 2026)*

One of the key principles of EU MAR is that inside information must be disclosed as soon as possible when it arises, unless the issuer satisfies certain strict requirements allowing it to delay disclosure (see "*Revised conditions for delayed disclosure of inside information*" below).[11] This is a sensitive issue in so-called "protracted processes", such as acquisitions, where inside information may crystallize at different stages. In such circumstances, immediate disclosure of inside information may sometimes prejudice the issuer (*e.g.*, in the case of extended confidential negotiations) who may wish to keep certain information confidential. The approach under EU MAR is different than under the U.S. securities laws where companies can hold certain types of sensitive information for longer periods before triggering a disclosure obligation.

---

[10] Following Brexit, EU MAR no longer directly applies in the UK, but substantially equivalent provisions have been onshored into UK domestic law. See "*Potential impact for UK issuers*" below.

[11] In such a case, a decision to delay disclosure is required for each new piece of information deemed to be sufficiently precise and of a price sensitive nature as to constitute inside information.

An important change introduced by the EU Listing Act is that disclosure of inside information related to intermediate steps in a protracted process will no longer be required where those steps are connected to bringing about or resulting in a non-final set of circumstances or event. Instead, the disclosure requirement will apply only to inside information related to the "final" circumstances or "final" event of the protracted process.[12]

In practice, this means that issuers will no longer have to choose between immediate disclosure or delayed disclosure in the initial stages of a particular project. This will be especially relevant for extended negotiations in the context of M&A transactions (including cross border M&A with an EU company as buyer or seller). Issuers will however still be obliged to ensure the confidentiality of any inside information. The prohibitions of insider dealing and unlawful disclosure of inside information will also continue to apply in full and the obligation to draw up insider lists will remain in place.

B. Revised conditions for delayed disclosure of inside information *(Effective: June 5, 2026)*

Under EU MAR, one key condition for issuers seeking to delay disclosure of inside information is that such a delay "*[…]is not likely to mislead the public*." Pursuant to the EU Listing Act, this requirement will be replaced with a new condition requiring that "*the inside information is not in contrast with the latest public announcement or other type of communication by the issuer […] on the same matter to which the inside information refers*"—which is generally perceived as a loosening of the criteria for delaying disclosure.

An important change introduced by the EU Listing Act is that disclosure of inside information related to intermediate steps in a protracted process will no longer be required where those steps are connected to bringing about or resulting in a non-final set of circumstances or event.

The purpose of this change is to increase legal certainty and allow for a consistent interpretation of the conditions required for an issuer to take the decision to delay disclosure. The new condition will allow issuers to conclude with greater certainty that delaying disclosure is an option, especially if the issuer has not previously communicated on the matter to which the inside information relates.

Nevertheless, this new condition leaves room for interpretation. The European Commission is empowered to adopt a delegated act to set out a non-exhaustive list of such situations, which will likely be instrumental in ensuring the uniform application of this new criterion.

C. Market sounding regime: an optional safe harbor *(Effective: December 4, 2024)*

The EU Listing Act explicitly confirms that the market sounding regime is an optional safe harbor and not a mandatory procedure.[13]

As a result, disclosing market participants (DMPs) can decide whether or not to comply with the information and record-keeping requirements of the market soundings regime when gauging market interest. If they do, they will benefit from the statutory safe harbor. However, if they do not, they may still demonstrate the market sounding was carried out in the normal exercise

[12] The European Securities and Markets Authority (ESMA) has launched a consultation to gather feedback on the changes introduced by the EU Listing Act, including on non-exhaustive lists of (i) the protracted process and the moment of disclosure of the relevant inside information; (ii) examples where there is a contrast between the inside information to be delayed and the latest public announcement by the issuer. ESMA will review all feedback received and expects to deliver its final technical advice to the European Commission by April 30, 2025.

[13] "Market soundings" are communications of information to one or more potential investors prior to the announcement of a transaction, in order to gauge the interest of such potential investors in the possible transaction and its conditions, such as its potential size or pricing. These communications can be done by an issuer, a secondary offeror, or a third party acting on behalf of any of such persons.

of a person's employment, profession or duties and will thus not be presumed to have unlawfully disclosed inside information. In such cases, DMPs remain nevertheless obliged to specifically assess whether the market sounding will involve the disclosure of inside information and make a written record of their conclusion.

D. Higher thresholds and new exemptions for managers' transactions *(Effective: December 4, 2024)*

The Listing Act also introduced two important changes to the regime applicable to transactions by persons discharging managerial responsibilities (PDMRs) and their closely associated persons (CAPs):

- **Higher thresholds**. The threshold to notify the issuer and National Competent Authorities of transactions made by PDMRs and CAPs has been increased from €5,000 to €20,000. That being said, National Competent Authorities from EU Member States are allowed to increase the new threshold further to €50,000, or to decrease it to €10,000.

- **New exemptions**. The exemptions for transactions that PDMRs may conduct during a closed period[14] have been expanded as follows:

  - the exemption regarding employee share schemes has been broadened to include employee schemes that relate to financial instruments other than shares; and

  - a new exemption for trading during closed periods has been introduced based on the rationale that the PDMR trading prohibition should only cover transactions that result from active investment decisions made by the PDMR. We believe this is a positive development as it will provide greater certainty to PDMRs who may otherwise have concerns that they could violate EU MAR as a result of "passive" trades (*e.g.*, a discretionary asset management mandate executed by an independent third party).

E. More proportionate administrative sanctions *(Effective: June 5, 2026)*

The EU Listing Act will make sanctions for violations of disclosure requirements more proportional to the size of the issuer. As a general rule, pecuniary sanctions for this type of violation will, subject to certain exceptions, be calculated as a percentage of the total annual turnover of the issuer.

Now a few years following Brexit, the rules governing capital markets in the EU and the UK are growing increasingly apart.

Potential Impact For UK Issuers

Following the expiration of the Brexit transition period, the EU MAR framework ceased to apply to financial instruments admitted to trading on UK listing venues. However, the version of EU MAR applicable at the time was "onshored" and became part of UK domestic law (UK MAR). Until the EU Listing Act was adopted, EU MAR and UK MAR were largely aligned, which made it relatively easy for issuers to manage their obligations under both regimes. The revisions to EU MAR introduced by the Listing Act usher an era of greater divergence between the two regimes, in particular as a result of the new rules adopted in the EU in respect of any "protracted processes." As a result, UK issuers with securities listed both in the UK and in the EU will have to comply with two different sets of rules to manage the same non-material public information and should prepare to adjust their existing processes accordingly. Further amendments to UK MAR are also expected in the coming year(s).

[14] MAR prohibits trading by PDMRs during a period of 30 calendar days before their company's announcement of its annual and (mandatory) interim financial reporting (so-called "closed periods"), unless certain stringent conditions are met, and the issuer allows such trade.

We believe this is part of a broader trend whereby, now a few years following Brexit, the rules governing capital markets in the EU and the UK are growing increasingly apart, most notably, in the UK, as a result of the finalisation[15] of the new UK listing rules in July 2024[16] and the recent publication by the UK Financial Conduct Authority (FCA) of a far reaching consultation paper on proposed reforms to the UK prospectus regime.[17]

Reforms to the UK prospectus regime (including rules regarding the content and publication of prospectuses) under the Public Offer and Admissions to Trading Regulations are currently subject to consultation. New rules are expected to be finalised by the end of H1 2025 (subject to FCA approval) and to apply from late H2 2025. However, certain proposals already diverge significantly from the position under the EU Listing Act. For example, in the UK, it is currently proposed to raise the prospectus exemption threshold for secondary offerings and admissions to trading on a regulated market to 75%, in comparison to the 30% exemption threshold introduced by the EU Listing Act (see "*Key Changes to EU PR*" below). The other exemptions for fungible issuances have not been used widely in the UK debt market due to the ubiquity of the base prospectus format so it is unlikely to have a significant impact on UK issuers. The true level of divergence between the UK and EU capital markets regimes will only become clear once the new UK prospectus rules crystallize next year.

Key Changes To EU PR

In addition to the EU MAR changes discussed above, the EU Listing Act also introduced a number of key changes to EU PR,[18] which are summarized below.

[15] For additional information, see our prior memorandum published in July, available here.

[16] FCA Policy Statement (PS24/6), "Primary Markets Effectiveness Review: Feedback to CP23/31 and final UK Listing Rules" (July 11, 2024), available here.

[17] FCA (CP24/12), "Consultation on the new Public Offers and Admission to Trading Regulations regime" (July 26, 2024), available here.

[18] The Prospectus Regulation sets out the requirements for the drafting, approval, and dissemination of the prospectus to be published in the event of a public offering or admission to trading on a regulated market located or operating within an EU Member State.

A. Expanded and additional exemptions from the obligation to publish a prospectus *(Effective: December 4, 2024)*

- **Prospectus Publication Exemption**. A dual-threshold system now applies, *i.e.*, below the threshold of either €12million (the principal threshold, increased from €8million) or €5million, offers of securities to the public will be exempted from the obligation to publish a prospectus, provided the offers do not require passporting.

- **Fungible Securities Exemption**. The exemption from the obligation to publish a prospectus for the admission to trading only (*i.e.*, not involving a public offer) of fungible securities has been extended to apply to public offers, and the threshold for this exemption is raised from 20% to 30%, subject to certain conditions.[19]

- **New Fungible Securities Exemption**. A new exemption for both public offers and admissions to trading of securities fungible with other securities already admitted to trading for at least 18 months, regardless of size, subject to certain conditions.[20]

B. Streamlining prospectus content requirements

Two new simplified prospectus formats (Effective: March 5, 2026). The EU Listing Act introduces two new, simplified types of prospectuses:

- "EU Follow-on prospectus" for several categories of issuers with securities that have been admitted to trading on a regulated market for at least 18 months before the offer to the public and/or seeking admission to trading, or where the securities are fungible with such securities; and

[19] The issuer may not be subject to restructuring or insolvency proceedings and is required to file and publish a short-form document with key information for investors.

[20] The new securities may not be issued in connection with a takeover, merger or division, nor the issuer be subject to restructuring or insolvency proceedings. The issuer is also required to file and publish a short-form document with key information for investors.

- "EU Growth issuance prospectus" for small- and medium-enterprises that satisfy certain criteria.

The EU Follow-on prospectus will replace the current simplified disclosure regime for secondary issuances and EU recovery prospectuses under EU PR. The EU Growth issuance prospectus will have lighter content requirements than the current EU Growth Prospectus which it will replace.

Standardised and simplified prospectus disclosure (Most changes effective: June 5, 2026, unless becoming effective earlier). Key changes introduced by the EU Listing Act include the following:

- A standardised prospectus format is introduced for both equity and non-equity securities,[21] and prospectuses relating to equity securities shall be limited to a maximum of 300 pages. Prospectuses are required to be distributed in electronic format only and may (in certain cases) also be drafted in English only.
- Prospectuses may incorporate by reference an expanded list of documents, such as a universal registration document.
- Only two years of historical financial information will be required for an equity offering.
- Risk factors are also simplified, with the EU Listing Act clarifying that risk factors should not be generic and used as mere disclaimers and should be listed in a manner that reflects their significance, as determined by the issuer.
- Debt/non-equity prospectuses only:
  - Issuers are now able to forward-incorporate annual or interim financial information, if it is within the 12-month period for which a base prospectus is valid.[22]
  - Supplements to a base prospectus should not be used to introduce a new type of security for which the necessary information has not been included in the base prospectus.[23]
  - It should also be noted that withdrawal rights will be extended from two to three days following the publication of a prospectus supplement.
  - Prospectuses may incorporate by reference an expanded list of documents including, for example, an approved universal registration document (URD), sustainability reports included in management reports and the short-form document required for certain fungible exemptions referred to above.
  - An issuer will only be required to have a URD approved by a National Competent Authority for one year (reduced from two years) before subsequent URDs can be filed instead. URDs will also be excluded from the new rules relating to standardising prospectuses discussed above.
  - New prospectus content requirements will also be developed for EU Green Bond Standard prospectuses, aligned to requirements under the EU Green Bond Standard Regulation.

[21] ESMA is consulting on draft technical advice concerning the EU Prospectus Regulation. ESMA's consultation addresses the (i) content and format of prospectuses, including the additional information to be included in prospectuses for non-equity securities that are advertised as taking into account ESG factors or pursuing ESG objectives; and (ii) criteria for the scrutiny and the procedures for approval of prospectuses. ESMA will consider all feedback received and expects to publish final technical advice in Q2 2025.

[22] Annual updates will still be required to maintain listing, but a supplement will not be required for annual or interim financial information.

[23] ESMA intends to launch a consultation in Q1 2025 on draft guidelines specifying the circumstances in which a supplement will be considered to introduce a new type of security into a base prospectus.

Trade Controls: Recent Developments and Changes on the Horizon for 2025

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

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

Ana Carolina Maloney
Associate
Washington, D.C.
amaloney@cgsh.com

The second Trump Administration is expected to mark the return of a more transactional foreign policy approach, with an openness to dealmaking supported by the aggressive use (or threat) of trade controls. Boards should, therefore, expect the U.S. government to continue to rely on trade controls as a key foreign policy tool. Although specific actions remain uncertain, significant change is possible on a number of fronts, including sanctions relating to China, Russia, Iran, Syria and Venezuela.

2024 was an active year in U.S. trade controls against Russia and China in particular. In addition to the continued designations of individuals and entities, foreign financial institutions (FFIs) faced heightened secondary sanctions risks with respect to Russia, and companies dealing with semiconductors, microelectronics and other advanced technologies faced additional restrictions relating to China. Also, the statute of limitations for U.S. sanctions violations increased from five to ten years, exposing companies to greater enforcement risk for historical conduct.[1]

Russia

Over the past year, the Biden Administration has continued to impose sanctions to limit Russian-government sources of revenue in response to the war in Ukraine. For example, on April 1, 2024, the U.S., in coordination with the United Kingdom, issued new prohibitions on the import of Russian-origin aluminum, copper and nickel, and limitations

[1] For additional details, see our May blog post available here.

with respect to their use on global metal exchanges and in over-the-counter derivatives trading.[2] The U.S. government also tightened sanctions in the financial sector on a number of fronts. These include blocking sanctions against additional entities in the Russian financial sector, including Gazprombank (the largest and most significant remaining non-sanctioned Russian bank that processed payments for Russian gas sold to third countries since spring 2022) and the National Settlement Depositary, the Russian central securities depository, as well as the expansion of secondary sanctions against FFIs for engaging in certain transactions or services with parties blocked under post-2021 Russia-related sanctions.[3] More recently, the Biden Administration has in its final days imposed sanctions targeting the Russian energy sector, including blocking sanctions against certain Russian oil companies, oilfield service providers, maritime insurance providers and more than 180 so-called "shadow fleet" vessels.

As the war in Ukraine enters its fourth year with a new U.S. administration entering office, the status of Russia sanctions going forward will likely depend on the prospects of a negotiated settlement to the war in Ukraine. Although the continued imposition of sanctions cannot be ruled out in view of a negotiated resolution, we do not expect a wholesale rollback of sanctions in the short term, which could be met with potential U.S. congressional action. However, a change in the pace and volume of new sanctions along with targeted authorizations are more likely. Notwithstanding increased coordination between U.S., UK and EU sanctions authorities in recent years in connection with Russia-related sanctions (including a new memorandum of understanding between the U.S. Department of the Treasury, Office of Foreign Assets Control and the UK Office of Financial Sanctions Implementation for information sharing), greater divergence in the imposition and enforcement of sanctions should not be ruled out in the future.

China

In 2024, the U.S. continued to impose a number of trade control measures against China, in particular relating to the Chinese military-industrial complex, export controls relating to sensitive technologies and inbound and outbound investment restrictions.[4] For further discussion, *see* FDI Regimes Ramp up Globally and Enhance Enforcement; U.S. Outbound Investment Regime Goes into Effect. Most recently, and in the final weeks of the Biden Administration, the U.S. Department of Commerce and Bureau of Industry and Security introduced extensive export controls against China relating to semiconductor manufacturing equipment, software tools for developing semiconductors and high-bandwidth memory (which are critical for AI and advanced computing integrated circuits), as well as additional controls on advanced computing AI technology, including advanced computing chips and closed AI model weights.

In 2025, boards of directors should continue to expect additional trade restrictions against China, including potential updates to the Trump-era Chinese military companies sanctions program, which remained relatively dormant during the Biden Administration. Although we expect trade controls to remain focused on targets relating to the Chinese military-industrial complex and sanctions evasion, third-party commercial actors could be indirectly impacted in sectors in which Chinese products may have both military and commercial non-military applications, such as shipbuilding, drone manufacturing, robotics and other advanced or critical technologies. Boards of directors should, therefore, also be prepared for more targeted and novel sanctions in relation to China, including the potential escalation of sanctions and export controls in conjunction with other trade restrictions, such as tariffs and the new outbound investment regime. China, in turn, may be expected to increase its use of countermeasures against western companies, such as the imposition of sanctions against a U.S. drone manufacturer in October 2024 and export controls against a number of U.S. defense companies in January 2025.

[2] For additional details, see our April blog post available here.

[3] For additional details, see our November alert memo and December blog post available here and here.

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

Other Countries

Boards of directors should also be prepared for sanctions developments in response to the geopolitical situation in a number of other countries, including Syria, Iran, Venezuela and Cuba. Following the fall of the Assad regime, the Biden Administration issued an expanded general license authorizing additional sanctions relief for basic human needs in Syria. However, Syria remains subject to comprehensive territory-wide U.S. sanctions and it remains to be seen what conditions the Trump Administration may place for the removal of sanctions.

With respect to Iran, the first Trump Administration pursued a maximum-pressure campaign, including withdrawal from the Iran nuclear deal and the imposition of additional sanctions. Although the more aggressive use of secondary sanctions targeting Iran's oil sales and distribution channels is possible, the geopolitical situation relating to Iran remains fluid in light of recent events in the region.

Following the deterioration of the electoral process in Venezuela, in the spring of 2024, the U.S. allowed a general license relating to the Venezuelan oil and gas sector to expire. Absent an improvement in U.S.-Venezuela relations or the political situation in Venezuela following the contested presidential elections, additional sanctions in Venezuela also remain possible. Sanctions and sanctions enforcement in relation to Cuba are also subject to potential change with the expected high-level appointments by President-elect Trump of several long-standing critics of the Cuban regime.

Boards of directors should also be prepared for sanctions developments in response to the geopolitical situation in a number of other countries.

Conclusion

In 2025, boards of directors should continue to evaluate their company's compliance posture in light of sanctions, export controls and geopolitical developments across jurisdictions. Boards should also be aware of the possibility of increased inconsistencies and potential conflicts across jurisdictions, including potential countermeasures from sanctioned jurisdictions.

clearygottlieb.com

Founded in 1946 by lawyers committed to legal excellence, internationalism, and diversity, Cleary Gottlieb Steen & Hamilton LLP is a leading international law firm with approximately 1,100 lawyers around the world. The firm has 16 closely integrated offices in New York, Washington, D.C., Paris, Brussels, London, Frankfurt, Cologne, Rome, Milan, Hong Kong, Beijing, São Paulo, Abu Dhabi, Seoul, and the Bay Area.

Under the rules of certain jurisdictions, this may constitute Attorney Advertising. Prior results do not guarantee a similar outcome.

Throughout this brochure, "Cleary Gottlieb", "Cleary" and the "firm" refer to Cleary Gottlieb Steen & Hamilton LLP and its affiliated entities in certain jurisdictions, and the term "offices" includes offices of those affiliated entities.

© 2025 Cleary Gottlieb Steen & Hamilton LLP

24.1209.02_011625