



Nordic Newsletter

July 2024

COVINGTON

BEIJING BOSTON BRUSSELS DUBAI FRANKFURT JOHANNESBURG LONDON
LOS ANGELES NEW YORK PALO ALTO SAN FRANCISCO SEOUL SHANGHAI WASHINGTON

www.cov.com

Editors' Note

Welcome to the third issue of Covington's Nordic Newsletter! This issue contains a discussion of the U.S. Treasury Department's enhancement of the U.S. Committee on Foreign Investment in the United States (CFIUS) enforcement in the context of unnotified transactions, mitigation agreement negotiations, and the imposition of civil monetary penalties.

Following on the Covington Nordic global series and webinar discussion of artificial intelligence regulatory frameworks, this issue provides an overview of the AI landscape in the Asia-Pacific region, as well as updates on artificial intelligence, connected and automated vehicles, and data privacy and cybersecurity matters.

Importantly for many of our clients and contacts in the Nordics, the U.S. Federal Trade Commission recently issued a final rule purporting to ban non-compete restrictions imposed on U.S. employees. Make sure not to miss key recommendations from Covington's leading antitrust and employment lawyers on how to address this development.

In the Autumn, we will host the next episode of the Nordic webinar series, "Recent Developments in Nordic and U.S. Cross Border M&A." That discussion will cover recent trends, the impact of key regulatory and compliance developments, and opportunities to leverage U.S. incentives to attract investments. The date and time of the webinar will follow.

Covington's Nordic Initiative keeps growing and thriving! Our people are key to our mission of delivering excellent work product to our valued clients with an efficient and cost-effective approach. For that reason, we happily welcomed Johan Dagergard to our London office. Johan is a dual-qualified New York and Swedish lawyer with extensive transactional and capital markets experience, and a deep understanding of the Nordic market. You can get to know Johan a little more in this newsletter.

We hope you enjoy a good read leading up to a delightful summer!

Best regards,

Barbara, Uri and Jared



Uri Doron
M&A, Private Equity
Partner, New York
+1 212 841 1042
UDoron@cov.com



Jared Manes
M&A, Private Equity
Partner, New York
+1 212 841 1054
JManes@cov.com



Barbara Asiain
M&A, Private Equity
Associate, New York
+1 212 841 1053
BAsiain@cov.com

[Jump to article](#)

<p>Spotlight Series on Global AI Policy — United States</p> <p style="text-align: right;">></p>	<p>Developments Under President Biden's Cybersecurity Executive Order</p> <p style="text-align: right;">></p>	<p>Overview of AI Regulatory Landscape in APAC</p> <p style="text-align: right;">></p>	<p>FTC Issues Final Rule Purporting to Ban Non-Compete Clauses with U.S. Workers</p> <p style="text-align: right;">></p>	<p>Treasury Department Moves to Enhance CFIUS's Enforcement Authorities</p> <p style="text-align: right;">></p>	<p>Two Updates Published by the UK FCA on the Anti- Greenwashing Rule, and the SDR and Labelling Regime</p> <p style="text-align: right;">></p>
--	--	---	---	--	--

Meet the Nordic Initiative: Johan Dagergard

Who is Johan Dagergard?

Just like Volvo Cars, I am of Swedish design, but increasingly under foreign influence after 12+ years in London and New York.

Tell us about your legal practice...

I am a dual-qualified New York and Swedish lawyer, part of Covington's Nordic Practice and based in the London office. My work is focused on corporate transactions, such as cross-border M&A and capital markets matters.

Trends and recent developments in the region?

One I will keep my eyes on is defence tech. With conflicts ongoing around the world and following Sweden's and Finland's NATO membership, this area is moving up in priority for technology companies and other innovators as well as for investors.

What inspired you to become a lawyer?

It seemed easier than becoming a professional golfer... I was also attracted by the systematic approach to problem-solving, which is central in the legal education and a skill that is useful for any type of career.

What do you like the most of advising Nordic-based clients?

They are mostly very bright with global ambitions and successes, yet maintaining friendly and positive attitudes and listening to advice.

How does a day in your life look like?

We had our first kid five months ago so life looks very different these days. I love to catch his wake-up before I head into the office. The commute is made bearable



by finding a seat on the tube, a good podcast and a rare rain-free morning. In the office I handle emails, calls and other work, while also trying to do at least one business development activity every day. Back home, I am hoping to make bath-time with the little one, followed by dinner with my wife and a Champions League game on TV while finishing up remaining work.

Your go-to Nordic restaurant / dish

Adam / Albin in Stockholm is one of my favorite restaurants anywhere, not only in the Nordics.

Favorite Nordic movie / music band

All the Sällskapsresan-movies. They are now available on Netflix with English subtitles, much to the joy of my American wife who had to sit through them all.

Ideal Nordic holiday

So many! Stockholm's archipelago, Österlen in the southeast parts of Skåne, the island of Gotland or the mountains in northern Sweden.

Licorice or kanelbulle?

Kanelbulle, hands down. I'm something as rare as a licorice-hating Swede.



Spotlight Series on Global AI Policy

U.S. Tech Legislative, Regulatory & Litigation Update

This article highlights key legislative, regulatory, and litigation developments in the first quarter of 2024 related to artificial intelligence (“AI”), connected and automated vehicles (“CAVs”), and data privacy and cybersecurity. As noted below, some of these developments provide industry with the opportunity for participation and comment.

- 1 Artificial Intelligence**

- 2 AI Litigation Developments**

- 3 Connected & Automated Vehicles**

- 4 Data Privacy & Cybersecurity**



1 Artificial Intelligence

Federal Legislative Developments

AI remained a focal point for Congress this quarter. Multiple bills proposing to regulate AI were introduced, covering issues such as antitrust, transparency, and training data, and House leadership created a bipartisan task force to address AI regulation.

- **Antitrust:** Some bills introduced this quarter relate to the potential impact of AI on competition. For example, in January, Senator Klobuchar (D-MN) introduced the [Preventing Algorithmic Collusion Act of 2024](#) (S. 3686). The Act would create a presumption that a defendant entered into an agreement, contract, or conspiracy in restraint of trade in violation of the antitrust laws if the defendant: (i) distributed a pricing algorithm to two or more persons with the intent that the pricing algorithm be used to set or recommend a price or (ii) used a pricing algorithm to set or recommend a price or commercial term of a product or service and the pricing algorithm was used by another person to set or recommend a price. The Act also would require companies using algorithms to set prices to provide transparency and would prohibit the use of “nonpublic competitor data” to train any pricing algorithm.
- **Transparency:** Other bills focus on transparency requirements for AI. For instance, in March, Representative Eshoo (D-CA-16), along with 3 bipartisan co-sponsors, introduced the [Protecting Consumers from Deceptive AI Act](#) (H.R. 7766). The Act would direct the National Institute of Standards and Technology (“NIST”) to facilitate the development of standards for identifying and labeling AI-generated content, including through technical measures such as provenance metadata, watermarking, and digital fingerprinting. The Act also would require generative AI developers to include machine-readable disclosures within audio or visual content generated by their AI applications. Providers of covered online platforms would have to implement the disclosures to label AI-generated content.
- **Consent for Training Data:** Legislative proposals also focus on consent for use of training data. For example, Senators Welch (D-VT) and Lujan (D-NM) introduced the [Artificial Intelligence Consumer Opt-in, Notification, Standards, and Ethical Norms for Training Act or the “AI CONSENT Act”](#) (S. 3975). The Act would require entities to receive an individual’s express informed consent before using “covered data” (defined broadly) to train an AI system.
- **AI Task Force:** This quarter, House Speaker Mike Johnson (R-LA-4) and Minority Leader Hakeem Jeffries (D-NY-8) [announced](#) the establishment of a bipartisan Task Force on AI. Speaker Johnson and Leader Jeffries have each appointed 12 members to the Task Force. Among other things, the Task Force will produce a comprehensive report that will include: (i) guiding principles; (ii) forward-looking recommendations; and (iii) bipartisan policy proposals.

Federal Regulatory Developments

- **National Science Foundation (“NSF”):** The NSF [announced](#) the launch of the [National AI Research Resource \(“NAIRR”\)](#), a two-year pilot program that will support AI researchers and aid innovation. NSF will partner with ten other federal agencies as well as 25 private sector, nonprofit, and philanthropic organizations to power AI research and inform the design of the full NAIRR ecosystem over time. Specifically, the NAIRR pilot will support research to advance safe, secure, and trustworthy AI, as well as the application of AI to challenges in healthcare and environmental and infrastructure sustainability. The NAIRR launch meets a goal outlined in the White House’s October 2023 Executive Order on the Safe, Secure, and Trustworthy Development and Use of AI (“EO”), which directs NSF to launch a pilot for the NAIRR.
- **Department of Commerce:** The Department of Commerce [published](#) a [proposed rule](#) to require providers and foreign resellers of U.S. Infrastructure-as-a-Service products to, among other things, notify the Department of Commerce when a foreign person transacts with that provider or reseller to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity. The AI provisions of the proposed rule stem from mandates in the EO on AI. *Comments are due by April 29, 2024.*
- **Federal Communications Commission (“FCC”):** The FCC [released](#) a [declaratory ruling](#) stating that under the Telephone Consumer Protection Act (“TCPA”), telemarketing calls using an artificial or prerecorded voice simulated or generated through AI technology can be made only with the prior express written consent of the called party unless an exemption applies. The declaration followed the submission of reply comments supporting the change by the Attorneys General of 25 states and the District of Columbia. Further, the FCC [announced](#) that it will relaunch the Consumer Advisory Committee (“CAC”) to focus on emerging AI technologies and consumer privacy issues.
- **Federal Trade Commission (“FTC”):** The FTC issued a [supplemental Notice of Proposed Rulemaking \(“NPRM”\)](#) that would amend the Rule on Impersonation of Government and Business (“Impersonation Rule”) to prohibit the impersonation of individuals using AI and extend liability for violations of the Impersonation Rule. *Comments are due by April 30, 2024.* Additionally, the FTC [published](#) a blog post warning AI companies that it may be unfair and deceptive to quietly change their terms of service to adopt more permissive data practices, such as using consumers’ data for AI training, without adequate notice to consumers.
- **White House Office of Management and Budget (“OMB”):** OMB [issued](#) its first government-wide [policy memorandum](#) on deploying AI in the federal government

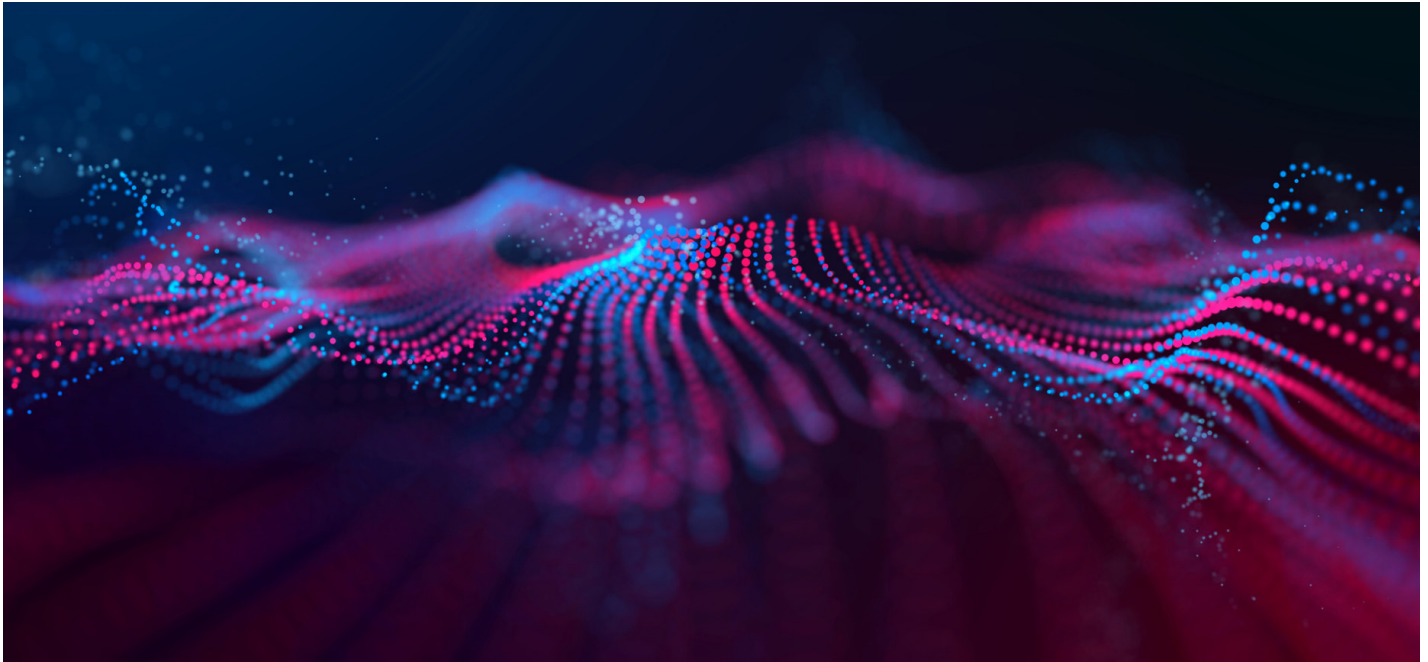
and managing its risks. The memorandum establishes requirements and guidance for federal agencies that aim to strengthen AI governance, advance responsible AI innovation, and manage AI risks, especially those risks that affect the rights and safety of the public. For example, the memorandum requires agencies to implement minimum governance procedures for certain rights-impacting and safety-impacting AI use cases.

- **U.S. Patent and Trademark Office (“USPTO”):** The USPTO [published](#) a guidance declaring that while AI systems and other “non-natural persons” cannot be listed as inventors in patent applications, the use of an AI system by a natural person does not preclude a natural person from qualifying as an inventor. Further, the person using the AI must have contributed significantly to the invention; simply overseeing an AI system’s creation is not sufficient. Those seeking patents must disclose if AI was used during the invention process. In conjunction with the guidance, the USPTO issued [examples](#) to illustrate the application of the guidance in specific situations. *Comments on the guidance and examples are due by May 13, 2024.*

2 AI Litigation Developments

Plaintiffs continue to test theories in lawsuits against companies developing AI models, with a number of suits focused on copyright infringement and related claims. The defendants in the copyright cases have responded by arguing, among other things, that the plaintiffs failed to plead facts establishing that models were trained on materials covered by copyright registrations, failed to support claims that the model is both an infringing “copy” and “derivative” of each registered work on which it was allegedly trained, and failed to identify copyright management information (“CMI”) that the defendants allegedly altered or removed. 2024 Q1 litigation developments include, for example:

- **New Copyright Complaints:** On March 8, a group of book authors brought a direct copyright infringement claim against Nvidia, alleging that Nvidia copied and used their copyright-protected works to train their NeMo Megatron series of LLMs. *Nazemian et al. v. Nvidia Corp.* 24-cv-1454 (N.D. Cal.). The same day, the authors also brought a copyright infringement suit against MosaicML for direct infringement and Databricks, Inc. for vicarious infringement concerning the training of Mosaic’s MPT LLM model series, including MPT-7B and MPT-30B. *O’Nan et al. v. Databricks Inc. et al.*, 3:24-cv-01451 (N.D. Cal.).
- On February 28, two suits were filed by news media organizations against OpenAI, alleging that OpenAI violated the Digital Millennium Copyright Act by training the ChatGPT LLM with copies of their works from which content management information had been removed. *Raw Story Media, AlterNet Media v. OpenAI, et al.*, 24-cv-1514 (S.D.N.Y.); *The Intercept Media, Inc. v. OpenAI, Inc. et al.*, 1:24-CV-01515 (S.D.N.Y.). The Intercept also named Microsoft as a defendant.
- On January 5, a class action complaint was filed by journalists and authors of nonfiction works against Microsoft and OpenAI alleging that the companies unlawfully reproduced their copyrighted works for the purpose of training their LLMs and ChatGPT. *Basbanes v. Microsoft*, 1:24-cv-84 (S.D.N.Y.). The *Basbanes* suit has since been consolidated with *Authors Guild, et al., v. Open AI Inc., et al.*, 23-cv-08292 (S.D.N.Y.) and *Alter, et al., v. Open AI Inc., et al.*, 23-cv-10211 (S.D.N.Y.).
- **Responses in New York Times Case:** On February 26, OpenAI filed a motion to dismiss in *The New York Times Company v. Microsoft et. al.* 1:23-cv-11195 (S.D.N.Y.), arguing, among other things, that NYT failed to allege that OpenAI had actual knowledge of specific acts of infringement for the purposes of contributory copyright liability and that NYT failed to identify the CMI that OpenAI allegedly removed. On March 3, Microsoft filed a partial motion to dismiss, arguing, among other things, that NYT failed to state a claim against Microsoft for contributory infringement for failure to allege an underlying direct infringement by end users and that NYT cannot allege Microsoft’s actual knowledge of (or willful blindness to) any act of direct infringement. On March 11 and March 18, NYT responded to both motions to dismiss, making procedural arguments and arguing, among other things, that OpenAI had knowledge of contributory infringement because NYT had actually informed OpenAI of this alleged infringement. Though fair use arguments are not being litigated at this stage, both parties have discussed fair use case law in their briefing.
- **Copyright Management Information (“CMI”) Dismissals in GitHub Case:** On January 3, the court in *Doe v. GitHub*, 22-cv-6823 (N.D. Cal.) issued its second decision on a motion to dismiss, partially granting and denying the motion for six of the plaintiffs’ eight claims. The court found that some of the plaintiffs sufficiently alleged Article III standing to seek damages based on amended allegations that included examples of their code that were output by the Copilot coding tool. The court also found that certain state law claims were preempted by the Copyright Act and dismissed them with prejudice. The court also dismissed the plaintiffs’ CMI claims under the Digital Millennium Copyright Act with leave to amend, holding that the claims at issue lie only when CMI is removed or altered from an *identical* copy of a copyrighted work, and the amended complaint only identified examples of outputs that were alleged to be modifications of copyrighted code, and not identical copies. On January 25, the plaintiffs filed a second amended complaint, re-alleging the CMI claims and bringing two breach of contract claims for open-source license violations and selling licensed materials in violation of Github’s policies. On February 28, defendants Microsoft



and Github moved to dismiss again, arguing that the plaintiffs still failed to plead that CMI was removed from identical copies of the plaintiffs' works.

▪ **Response to Amended Complaint in Google Case:**

On January 5, the plaintiffs in *Leovy v. Google LLC*, 3:23-cv-03440 (N.D. Cal) amended their complaint to name the plaintiffs, allege different causes of action, and plead additional allegations concerning Google's alleged violations of the plaintiffs' rights under property, privacy, and copyright law, among other things. On February 9, the defendant moved to dismiss the plaintiffs' amended complaint with prejudice. With respect to the plaintiffs' web scraping claims, the defendant argued, "outside copyright law (including its protection for fair use), there is no general right to control publicly available information." The defendant argued that the plaintiffs' direct copyright infringement claims based on generative AI output should be dismissed because the plaintiff pled that "Bard's output necessarily infringes the copyrights in all the works Bard trained on" without providing any examples of a "substantially similar" infringing output. The motion did not argue for dismissal of the direct copyright infringement claim based on the training process. With respect to the plaintiffs' negligence claims, the defendant argued that the plaintiffs failed to adequately allege that it owed the plaintiffs a duty of care and that the economic loss rule otherwise barred a negligence claim.

▪ **Dismissals and Consolidation in N.D. Cal Litigation:** On February 12, in a consolidated opinion, the court granted the defendants' motions to dismiss the claims in *Tremblay et al. v. OpenAI, Inc. et al.*, 3:23-cv-03223 (N.D. Cal.) and

those in the related case of *Silverman, et al v. OpenAI, Inc., et al.*, 23-cv-03416 (N.D. Cal.) case for vicarious infringement, violation of the Digital Millennium Copyright Act, and negligence, with leave to amend. The court also dismissed the plaintiffs' unjust enrichment claim with prejudice, but allowed the unfair competition claim to proceed. The case was subsequently consolidated on February 16 with the *Silverman* case and *Chabon v. OpenAI, et al.*, 23-cv-04625 (N.D. Cal). On March 13, the plaintiffs filed a first consolidated amended complaint (under the new caption, "*In Re ChatGPT Litigation*"), narrowing to two counts of direct copyright infringement and violation of the California Unfair Competition Act.

▪ **Right of Publicity Complaint:** On January 25, representatives of comedian George Carlin's estate filed suit in *Main Sequence, Ltd. et. al. v. Dudesy, LLC*, 24-cv-711 (C.D. Cal.), alleging that the defendants, by training an AI model to mimic Carlin's stand-up performances and by publishing the allegedly AI-created "George Carlin Special," have unlawfully used Carlin's name, image and likeness without consent, in addition to infringing copyrighted Carlin materials. There is some uncertainty expressed in the complaint as to whether the "George Carlin Special" was produced using a generative AI model or involved a human-written script paired with assistive tools such as an AI voice generator. The plaintiffs allege that in either case, Carlin's image and likeness was unlawfully used and his reputation harmed.



3 Connected & Automated Vehicles

- Autonomous Vehicle Accessibility Act:** On January 30, Representatives Greg Stanton (D-AZ) and Brian Mast (R-FL), members of the House Transportation and Infrastructure Committee, introduced the bipartisan [Autonomous Vehicle Accessibility Act](#) (H.R. 7126). The Act is intended to help people with disabilities better access the mobility and independence benefits of ride-hail CAVs, such as by: (1) prohibiting states from issuing motor vehicle operator's licenses in a manner that prevents a qualified individual with an ADA disability from riding as a passenger in a vehicle equipped with an automated driving system that is operating in fully autonomous mode; and (2) requiring the Secretary of Transportation to conduct an accessible infrastructure study to determine the best practices for public transportation infrastructure to be modified to improve the ability of Americans with disabilities to find, access, and use ride-hail autonomous vehicles. The bill was referred to the Subcommittee on Highways and Transit on February 12, 2024.
- Focus on Data Privacy Practices of Vehicle Manufacturers:** On February 27, Senator Markey (D-MA) sent a [letter](#) to the FTC asking the FTC to investigate the data privacy practices of car manufacturers. Senator Markey noted that the responses automakers provided to his late 2023 [inquiry](#) "gave [him] little comfort" and that the companies' "ambiguity and evasiveness calls out for the investigatory powers of the FTC." The letter "urge[s] the [FTC] to use the full force of its authorities to investigate the automakers' privacy practices and take all necessary enforcement actions to ensure that consumer privacy is protected."
- Continued Attention on Connectivity and Domestic Violence:** As we reported in our [last update](#), the FCC has taken steps to increase its understanding of certain safety issues implicated by connected vehicles with respect to the potential for wireless connectivity and location data to negatively impact partners in abusive relationships. Continuing this focus, on February 28, the FCC issued a

[press release](#) reporting that Chairwoman Rosenworcel circulated a Notice of Proposed Rulemaking regarding how the agency can leverage existing law to ensure that car manufacturers and wireless service providers "understand the full impact of the connectivity tools in new vehicles and how these applications can be used to stalk, harass, and intimidate." If adopted, the NPRM "would seek comment on the types and frequency of use of connected car services that are available in the marketplace today." Among other things, the NPRM would ask if changes to the FCC's rules implementing the Safe Connections Act are needed to address the impact of connected car services on domestic abuse survivors. It also would seek comment on what steps connected car services can proactively take to protect survivors from the misuse of such services.

4 Data Privacy & Cybersecurity

Privacy

With respect to privacy, a number of states kicked off the new year with new privacy laws and the FTC continued to bring enforcement actions related to companies' privacy practices.

- New State Privacy Laws:** Legislatures in New Jersey, New Hampshire, and Kentucky passed new data privacy laws that largely resemble the approaches taken under existing privacy frameworks in the U.S. Maryland's legislature has also passed a comprehensive privacy law, although both chambers are working to reconcile differences. Additionally, Nebraska [enacted](#) a genetic privacy law regulating direct-to-consumer ("DTC") genetic testing companies. The law is one of a flurry of bills regarding DTC genetic testing that have been introduced in several states since the beginning of 2024, following the enactment of several DTC genetic testing laws in 2023.
- FTC Consent Orders:** The FTC recently announced proposed consent orders with [Outlogic and InMarket Media](#) related to the use of precise geolocation data. Both companies collect location data using software development kits ("SDKs") installed in first and third party apps, among other data sources. According to the FTC's complaints, Outlogic sold this data to third parties (including in a manner that revealed consumer's visits to sensitive locations) without obtaining adequate consent, and InMarket used this data to facilitate targeted advertising without notifying consumers that their location data will be used for targeted advertising. In both cases, the FTC alleged that these acts and practices constituted unfair and/or deceptive acts or practices under Section 5 of the FTC Act.

Cybersecurity

Federal cybersecurity regulators have had a busy start to 2024 and set in motion a number of new proposed rules and

cybersecurity standards that, if implemented, will redefine the landscape for federal cybersecurity regulations in the years ahead.

▪ **Critical Infrastructure Broadly Defined:** The U.S.

Cybersecurity and Infrastructure Security Agency (“CISA”) published a [proposed rule](#) to implement the cyber incident reporting requirements for critical infrastructure entities from the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (“CIRCA”). Notably, the proposed rule broadly defines critical infrastructure entities (pursuant to Presidential Policy Directive 21) across the 16 critical infrastructure sectors. In total, CISA estimates that over 300,000 entities would be covered by the rule. CIRCA has two cyber incident reporting requirements for covered critical infrastructure entities: a 24-hour requirement to report ransomware payments and a 72-hour requirement to report covered cyber incidents to CISA. Under CIRCA, the final rule must be published by September 2025.

- **Cybersecurity Framework 2.0:** The U.S. National Institute of Standards and Technology (“NIST”) [published](#) version 2.0 of its [Cybersecurity Framework](#). The new version incorporates some significant updates to the Framework including: expanded application (i.e., broad application regardless of cybersecurity program maturity); a new “govern” function (i.e., whether an organization’s cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored); increased focus on cybersecurity supply chain risk management (e.g., whether an organization performs due diligence on potential suppliers and monitors the relationship through the technology or service life cycle); and new reference tools.
- **Federal Cybersecurity Enforcement Action:** The U.S. Department of Health and Human Services Office of Civil Rights [announced](#) that it had settled a cybersecurity investigation with Montefiore Medical Center, a non-profit hospital system based in New York City, for \$4.75 million.



Jennifer Johnson
Technology and Communications
Regulation
Partner, Washington
+1 202 662 5552
JJohnson@cov.com



Nicholas Xenakis
Regulatory and Public Policy
Of Counsel, Washington
+1 202 662 5846
NXenakis@cov.com



Phillip Hill
Copyright and Trademark
Counseling and Prosecution
Special Counsel, New York
+1 212 841 1033
PAhill@cov.com



Jayne Ponder
Data Privacy and Cybersecurity
Associate, Washington
+1 202 662 5008
JPonder@cov.com



Shayan Karbassi
Regulatory and Public Policy
Associate, Washington
+1 202 662 5393
SKarbassi@cov.com



Olivia Dworkin
Regulatory and Public Policy
Associate, Los Angeles
+1 424 332 4817
ODworkin@cov.com



Jorge Ortiz
Data Privacy and Cybersecurity
Associate, Washington
+1 202 662 5721
JOrtiz@cov.com



Jemie Fofanah
Data Privacy and Cybersecurity
Associate, Washington
+1 202 662 5326
JFofanah@cov.com



Andrew Longhi
Antitrust and Commercial
Associate, Washington
+1 202 662 5511
ALonghi@cov.com



Lauren Gerber
Litigation and Investigations
Associate, Washington
+1 202 662 5517
LGerber@cov.com



Vanessa Lauber
Data Privacy and Cybersecurity
Associate, New York
+1 202 662 5897
VLauber@cov.com



Zoe Kaiser
Litigation and Investigations
Associate, San Francisco
+1 415 591 6019
ZKaiser@cov.com



Madeleine Dolan
Litigation and Investigations
Associate, Washington
+1 202 662 5300
MDolan@cov.com

Developments Under President Biden's Cybersecurity Executive Order

National Cybersecurity Strategy, and AI Executive Order - April 2024

This article is part of an ongoing series on the implementation of [Executive Order 14028, "Improving the Nation's Cybersecurity,"](#) issued by President Biden on May 12, 2021 (the "Cyber EO"). The [first article](#) summarized the Cyber EO's key provisions and timelines, and the subsequent blogs described the actions taken by various government agencies to implement the Cyber EO from [June 2021](#) through [March 2024](#). This article describes key actions taken to implement the Cyber EO, as well as the [U.S. National Cybersecurity Strategy](#), during April 2024. It also describes key actions taken during April 2024 to implement President Biden's Executive Order on [Artificial Intelligence](#) (the "AI EO"), particularly its provisions that impact cybersecurity, national security, and secure software.

NIST Publishes Initial Draft Handbook on Secure IOT Development

On April 3, NIST released an initial public draft of a [cybersecurity handbook](#) that outlines considerations for developing and deploying internet of things products across sectors. In sum, the handbook is intended to help outline and mitigate the risks that may be associated with these products. Among other things, the handbook outlines approaches to cybersecurity in IoT products, including with respect to architecture and deployment of the products. Among other topics and consistent with the government's focus on supply chain security, this handbook also addresses cybersecurity considerations relating to the hardware



and software components of IoT. The handbook also provides examples of implementation of these practices, including with respect to deployment.

New FAR Part 40 Established

On April 10, the FAR Council released a [Request for Information \(RFI\)](#) relating to the final FAR rule to establish FAR Part 40, which contains information and supply chain security requirements. That final rule was published in the Federal Register on April 1. The RFI is proposing a two-part test to determine whether a requirement should appear in the new Part 40. If the scope of a security requirement applies beyond information and communications technology (ICT), it should be placed in the new FAR Part 40. If the scope of the security requirement is limited to ICT, it would be located in current FAR Part 39 (“Acquisition of Information Technology”). The FAR Council is seeking comments on the contents of this FAR section through June 10, 2024.

NSA Issues Guidance on Safe Deployment of AI

On April 15, the National Security Agency’s Artificial Intelligence Security Center released guidance on [strengthening AI system security](#). The guidance is heavily focused on ensuring that known cybersecurity vulnerabilities in AI systems are appropriately mitigated, providing methodologies and controls to protect, detect, and respond to malicious activity against AI systems and related data and services, and improving the confidentiality, integrity, and availability of AI systems. The document is intended to be used by organizations that are deploying and operating externally developed AI systems on premises or in private cloud environments, especially those in high-threat, high-value environments.

DHS Collaborates with Open Source Foundation to Release New Tool for Creating and Translating SBOMs

On April 16, the Open Source Foundation collaborated with the Department of Homeland Security Science and Technology Directorate and the Cybersecurity and Infrastructure Security Agency (CISA) collaborated to develop a [new tool](#) that allows organizations, including government organizations, to read and generate Software Bills of Materials (SBOMs). The tool is open

source and therefore can be further developed as needs evolve. The tool, known as “protobom,” can be accessed and downloaded [here](#). It is unclear how this tool, and/or others, may be relied on by agencies as they implement the secure software development framework that we have written about [previously](#).

GAO Requests CISA to Produce List of Critical Software Identified By Federal Agencies Pursuant to Cyber EO

On April 18, the Government Accountability Office (GAO) issued a [report](#) which surveyed the states of implementation of the Cybersecurity Executive Order. In the report, GAO found that agencies had implemented 16 of the 17 requirements in Section 4 of the EO, which addresses enhanced mechanisms to ensure the integrity of the software used by federal supply chain partners. The report found that agencies had implemented 16 of the 17 requirements in Section 4, but highlighted action needed in one area. The report recommended, among other things, that CISA should issue its list of software and software product categories that are considered to be critical software, that CISA should direct Cyber Safety Review Board to document steps taken or planned to implement the recommendations provided to the President for improving the board’s operations, and that OMB should demonstrate that it has conducted cost analyses for the implementation of recommendations related to the sharing of threat information and resourcing needs for the implementation of an endpoint detection and response capability.

DOD Initiates Vulnerability Disclosure Program for Defense Contractors

On April 19, the Department of Defense (“DoD”) Cyber Crime Center (“DC3”) and Defense Counterintelligence and Security Agency (“DCSA”) announced a new [Defense Industrial Base Vulnerability Disclosure Program](#) (“DIB-VDP”).

The program stems from a pilot that DoD conducted for one year, and will allow program participants to be onboarded and integrated to allow for vulnerability threat assessment on those participants’ voluntarily identified assets and platforms.

CISA Issues Guidelines for Critical Infrastructure to Assess AI Risk

On April 29, the Cybersecurity Infrastructure Security Agency (“CISA”) released [guidelines](#) relating to security and safety

for use by critical infrastructure owners and operators. The guidelines outline the findings of CISA’s cross-sector analysis of AI risks, including cross-sector AI use cases and patterns in adoption. The analysis focuses on three risk types – attacks using AI, attacks that target AI systems, and failures in AI design and implementation. The guidelines that arose from this analysis are intended to mitigate the identified cross-sector AI risks to critical infrastructure.

NIST Issues Four AI Guidance Documents

On April 30, 2024, the National Institute of Standards and Technology (“NIST”) [issued](#) four significant guidance documents pursuant to the AI EO. These documents are: (1) a draft generative AI companion guide for NIST’s Secure Software Development Framework (SSDF) (2) a draft generative AI profile for NIST’s AI Risk Management Framework; a draft plan for global engagement on AI safety standards; and (4) draft guidance on “reducing risks posed by synthetic content.” Comments on each of these documents are due by June 2, 2024.

The draft generative AI companion guide for SSDF may prove to be the most impactful of these documents for government contractors. Federal agencies are currently required by OMB Memoranda M-22-18 and M-23-16 to obtain “self-attestation forms” from producers of certain “software” used by the agency that the software was



developed in compliance with certain principles in the SSDF. Such self-attestations are required for “critical software” by June 8, 2024, and for non-critical software by September 8, 2024. The term “software” is broadly defined to include almost all types of software, including products that contain software. Thus, contractors may already be required to provide SSDF attestations regarding AI products or services to the extent incorporated in or associated with “software” subject to the attestation requirements to the extent the NIST AI generative companion guide results in additional or different SSDF requirements for generative AI, such requirements may be incorporated into the SSDF attestation forms required from software producers.



Robert Huffman
Regulatory and Public Policy
Senior Of Counsel, Washington
+1 202 662 5645
RHuffman@cov.com



Ashden Fein
Regulatory and Public Policy
Partner, Washington
+1 202 662 5116
AFein@cov.com



Matthew Harden
Regulatory and Public Policy
Associate, New York
+1 212 841 1061
MHarden@cov.com



Susan Cassidy
Regulatory and Public Policy
Partner, Washington
+1 202 662 5348
SCassidy@cov.com



Ryan Burnette
Regulatory and Public Policy
Special Counsel, Washington
+1 202 662 5746
RBurnette@cov.com

Overview of AI Regulatory Landscape in APAC

With the rapid evolution of artificial intelligence (AI) technology, the regulatory frameworks for AI in the Asia–Pacific (APAC) region continue to develop quickly. Policymakers and regulators have been prompted to consider either reviewing existing regulatory frameworks to ensure their effectiveness in addressing emerging risks brought by AI, or proposing new, AI-specific rules or regulations. Overall, there appears to be a trend across the region to promote AI uses and developments, with most jurisdictions focusing on high-level and principle-based guidance. While a few jurisdictions are considering regulations specific to AI, they are still at an early stage. Further, privacy regulators and some industry regulators, such as financial regulators, are starting to play a role in AI governance.

This article provides an overview of various approaches in regulating AI and managing AI-related risks in the APAC region.

AI-Specific Laws and Regulations

Several jurisdictions in the region are moving toward AI-specific regulations, including the People’s Republic of China (hereinafter referred to as China), South Korea, and Taiwan.

- China has been most active in shaping regulations specific to generative AI technologies since 2023. It has taken a multifaceted approach that combines AI-specific regulations, national standards and technical guidance to govern generative AI services and the regulatory focus has been on services that are provided to the public in China. The [Interim Administrative Measures for Generative Artificial Intelligence Services](#) represent a milestone as the first comprehensive regulation specifically addressing generative AI services (a summary of this regulation can be found in our previous post [here](#)). Several non-binding technical documents and national standards have been issued or are being drafted to further implement this regulation. Prior to the regulation that specifically addresses generative AI services, China had issued regulations for [deep synthesis](#) and [algorithmic recommendations](#). Further, China promulgated [rules](#) on conducting an ethical review of scientific activities involving generative AI.
- Beyond a few provisions on narrow aspects scattered in other regimes, South Korea does not presently have a comprehensive AI-specific regulatory framework. Proposed in early 2023, the draft Act on Fostering the AI Industry and Securing Trustworthy AI remains currently pending before the National Assembly. If enacted, it would set out the first comprehensive legislative framework governing the usage of AI in South Korea, generally reflecting an approach that would permit AI usage and



developments subject to subsequent safeguards if and as needed.

- In parallel, the Personal Information Protection Commission (PIPC) has been advocating for a flexible approach to AI based on self-regulation, with support from the PIPC. Furthermore, the Korean Fair Trade Commission (KFTC) will soon start a detailed study to identify potential AI-induced risks in terms of consumer protection as well as unfair or anti-competitive practices, which might result in KFTC-supervised self-regulation of certain AI aspects through industry codes of conduct supplemented by a set of guidelines on AI, or even proposed legislation or amendments to existing consumer protection or antitrust rules.
- Similarly, Taiwan is drafting a basic law governing AI, i.e., the Basic Law for Development of Artificial Intelligence, which will set out fundamental principles for AI development and for the government to promote the development of AI technologies. However, it is still uncertain whether and when Taiwan will pass this draft law.

Non-binding AI Principles and Guidelines

Other jurisdictions in the APAC region take a voluntary approach for the moment, relying on non-binding principles and guidelines as well as existing laws to address AI-related issues. Such jurisdictions include Australia, Japan, Singapore, India, Hong Kong, Thailand and Vietnam.

For instance, Australia has so far taken a soft-law approach. Australia's [AI Ethics Principles](#) were published in 2019, setting out principles for certain aspects in relation to AI governance, including fairness, privacy protection and security, reliability and safety, transparency and explainability, and accountability. Similarly, Japan has no comprehensive AI-specific regulation but only provides non-binding guidance. Singapore, India, Hong Kong, Thailand and Vietnam also have their own AI-related guidelines.

In addition to non-binding guidelines, some regulators also provide practical tools for AI services. For instance, Singapore launched an [AI governance testing framework and toolkit](#) in May 2022 and the initiative of a generative AI evaluation sandbox in October 2023, providing a common baseline of evaluation testing methods and benchmarks to assess generative AI products.

In these jurisdictions that have not yet issued specific AI regulations, enforcement in relation to AI could be carried out under existing laws. For instance, in order to understand the implications of the development and use of AI on data privacy in Hong Kong, the privacy regulator of Hong Kong – the Office

of the Privacy Commissioner for Personal Data (PCPD) – [carried out compliance checks](#) on 28 organizations from August 2023 to February 2024 to understand their practices regarding the collection, use and processing of personal data in the development or use of AI, as well as their AI governance structure. Some jurisdictions have started to experiment with the best approach to regulate AI services, even though AI regulations are not in place yet. For instance, India's regulator – the Ministry of Electronics and Information Technology – [issued](#) a non-binding advisory on March 1, 2024, asking all AI tools (including AI models, software using generative AI or any algorithms) currently being tested, in development or are potentially unreliable, to seek approval from the government before being released to the public. However, the requirement mandating government approval of AI tools was soon withdrawn by an advisory [issued](#) later in that month.

The fast development of AI technologies certainly poses new regulatory challenges for APAC governments. With China being the first jurisdiction to adopt AI-specific regulations, there will still be uncertainties going forward regarding how other regulators in the APAC region will address the risks brought by AI. It will be sensible for companies that develop or deploy AI technologies in the APAC region to closely monitor these developments and be prepared.



Yan Luo
Data Privacy and Cybersecurity/
Antitrust / Competition
Partner, Palo Alto
+1 650 632 4705
YLuo@cov.com



Xuezi Dan
Corporate / Antitrust
Associate, Beijing
+86 10 5910 0518
XDan@cov.com



Laurie-Anne Grelier
Regulatory and Public Policy /
Antitrust / Competition
Special Counsel, Seoul
+82 2 6281 0005
LGrelier@cov.com

FTC Issues Final Rule Purporting to Ban Non-Compete Clauses with U.S. Workers

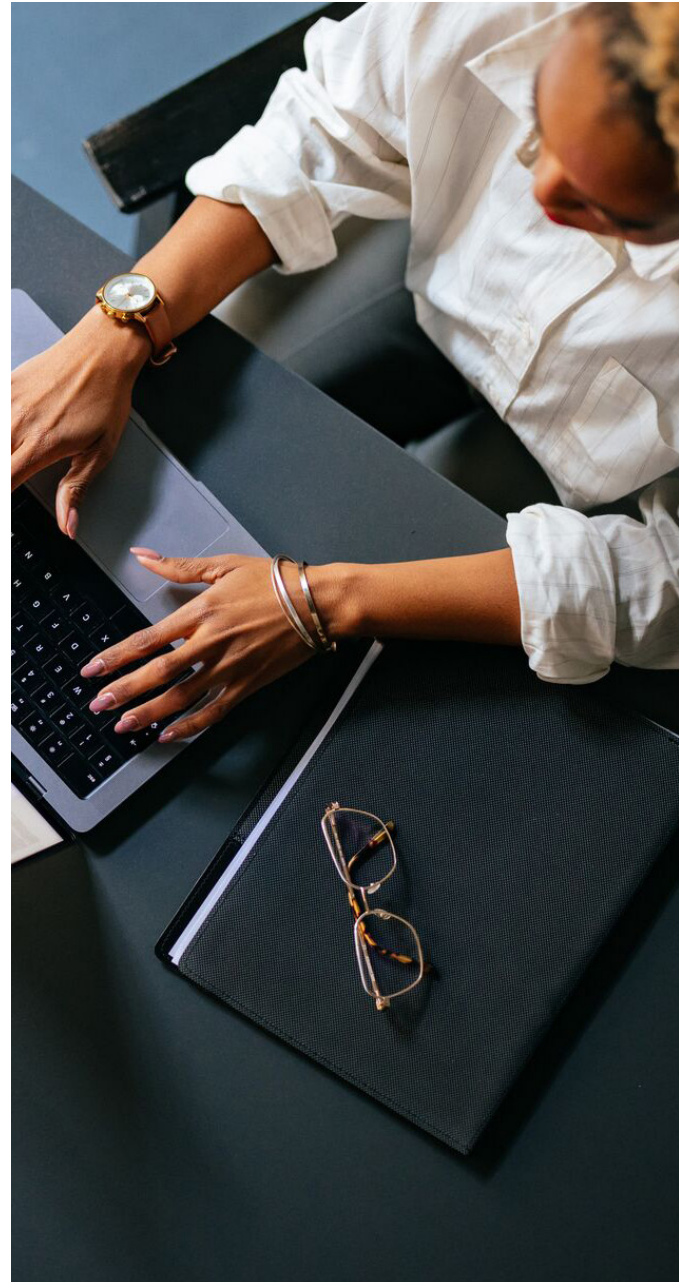
On Tuesday, April 23, during a special Open Commission Meeting, the Federal Trade Commission voted 3-2 to issue a [final rule](#) adopting what the FTC referred to as a “comprehensive ban on new non-competes with all workers.”^[1] The rule leaves intact non-competes entered into with “senior executives” before the rule’s effective date and carves out certain non-competes entered into pursuant to the sale of a business entity, ownership interest, or all or substantially all of a business entity’s assets. Once the final rule is published in the Federal Register, employers will have 120 days to comply, including by affirmatively rescinding any existing non-competes covered by the rule.

Publication of the final rule in the Federal Register will be the latest step in a process that began publicly on January 5, 2023, when the FTC [voted 3-1](#) to issue a Notice of Proposed Rulemaking. The FTC received more than 26,000 comments from members of the public and hosted a forum to discuss its proposed rule.

The FTC commissioners who voted in favor of the rule contend that the rule was properly promulgated pursuant to the FTC’s authority under Sections 5 and 6(g) of the FTC Act. Meanwhile, the dissenting FTC commissioners provided a roadmap of the expected court challenges on a variety of grounds, including with respect to whether the FTC has the statutory authority to issue competition-related rules (which numerous commentators have disputed), the constitutionality of the FTC’s non-compete ban (e.g., under the major questions doctrine), and the Administrative Procedure Act. It is an open question whether a court will stay the implementation of the non-compete ban pending the outcome of any such litigation.

The FTC’s Rule to Ban Noncompete Clauses

The final rule asserts that it is an unfair method of competition for a person (e.g., employer) to (1) enter into or attempt to enter into a non-compete; (2) enforce or attempt to enforce a non-compete; or (3) represent to a worker that the worker is subject to a non-compete. The rule would apply to all persons subject to the FTC’s jurisdiction and to all workers (i.e., any natural



person who works, whether paid or unpaid, including independent contractors, interns, volunteers)^[2] across the U.S. The final rule broadly defines a non-compete clause as “a term or condition of employment that *prohibits* a worker from, *penalizes* a worker for, or *functions to prevent* a worker from” seeking or accepting employment in the U.S. or operating a business in the U.S. after the conclusion of the worker’s service.

Significantly, the rule does not apply to a non-compete entered into by a person pursuant to a bona fide sale (i) “of a business entity,” or (ii) “of the person’s ownership

interest in a business entity,” or (iii) “of all or substantially all of a business entity’s operating assets.”^[3] The preamble to the final rule also notes that the rule does not categorically prohibit other types of restrictive covenants like NDAs and non-solicitation agreements. However, the FTC expressed the view that, if these types of covenants “function to prevent” a worker from seeking or accepting work or starting a business after they leave their job, such covenants could constitute non-competes under the final rule.

Non-competes entered into with “senior executives” before the effective date of the final rule are excluded from the ban. A “senior executive” is a worker who (1) was in a “policy-making position” and (2) received a total annual compensation of at least \$151,164 in the preceding year. The final rule defines “policy-making position” narrowly – as a business entity’s (a) president, CEO, or equivalent, or (b) any other officer^[4] or equivalent who has “policy-making authority.” “Policy-making authority” is the final authority to make policy decisions that control significant aspects of a business entity, excluding authority limited to advising or exerting influence.^[5] The FTC noted that this definition is a modified version of SEC Rule 3b-7.

The rule mandates that, within 120 days after publication of the rule, employers that have previously entered into non-competes covered by the rule must rescind the non-compete by providing clear and conspicuous notice to the worker that the non-compete is no longer in effect. Notice is not required with respect to eligible non-competes with “senior executives” or non-competes excluded from the rule (e.g., non-competes entered into pursuant to the sale of a business entity). The [final rule](#) published by the FTC contains a model notice (see page 566).

The Commission voted 3-2 to promulgate the final rule during an open commission meeting on April 23, 2024. Commission staff presented the empirical research they relied upon in connection with the non-compete ban. Chair Lina Khan and Commissioners Rebecca Kelly Slaughter and Alvaro Bedoya largely echoed the staff’s remarks. Commissioners Slaughter and Bedoya also noted that, while the rule would not apply to franchisee-franchisor agreements, such agreements are of particular interest to them.

Commissioners Melissa Holyoak and Andrew Ferguson dissented. Each questioned the FTC’s authority to promulgate the rule under Sections 5 and 6(g) of the FTC Act. The Commissioners also noted that *National Petroleum Refiners Association v. FTC*, on which the rule relies for support, fell out of favor decades ago. Commissioner Ferguson added that he believes that this rule presented a major policy question as it will nullify over 30 million contracts, redistribute half a trillion dollars, and affect nearly the entire economy.

In her final remarks, Chair Khan addressed the arguments of the dissenting Commissioners, contending that the

plain language of the FTC Act provides clear authority to promulgate this rule, courts have agreed with such an interpretation, and the Commission has used Section 6(g) authority for decades.



Takeaways

The rule is likely to be challenged in the near term. In the meantime, employers should take stock of their use of non-competes, including in current employment agreements, severance agreements, consulting agreements, IP assignment agreements, confidentiality agreements, employee handbooks, and equity award agreements, as well as in any past agreements where any such non-compete provisions are still effective.

Employers that use or are considering including non-compete clauses in arrangements with workers should consult antitrust and employment and executive compensation counsel. Employers will need to determine which of their workers are subject to non-compete clauses and determine whether they are required to provide notice of non-enforcement to those workers as required by the rule. This may include assessing whether a worker is a “senior executive” within the meaning of the rule.

The FTC has continued to aggressively enforce restrictions on labor mobility. With its vote to adopt the final rule on non-competes, the FTC will likely pursue enforcement actions against companies that it determines have violated the new rule after the 120-day grace period.



[1] The rule does not apply to entities over which the Commission does not have jurisdiction under the FTC Act, including certain banks, savings and loan institutions, federal credit unions, common carriers, air carriers and foreign air carriers, and persons subject to the Packers and Stockyards Act of 1921, as well as most non-profits.

[2] Worker does not include a franchisee in the context of a franchisee-franchisor relationship but does include a natural person who works for a franchisee or franchisor.

[3] The rule also does not apply where a cause of action related to

an existing non-compete clause accrued prior to the effective date. The preamble to the final rule notes that “This includes, for example, where an employer alleges that a worker accepted employment in breach of a noncompete if the alleged breach occurred prior to the effective date.”

[4] “Officer” means a president, vice president, secretary, treasurer or principal financial officer, comptroller or principal accounting officer, and any natural person routinely performing corresponding functions.

[5] “Policy-making authority” also excludes final authority to make such decisions for only a subsidiary or an affiliate of a common enterprise.



Lindsay Burke
Employment
Partner, Washington
+1 202 662 5859
LBurke@cov.com



John Graubert
Antitrust / Competition
Senior Counsel, Washington
+1 202 662 5859
JGraubert@cov.com



Terrell McSweeney
Regulatory and Public Policy /
Antitrust
Senior Of Counsel, Washington
+1 202 662 5126
TMcsweeney@cov.com



Evan Parness
Employment
Partner, New York
+1 212 841 1273
EParness@cov.com



Ryan Quillian
Regulatory and Public
Policy / Antitrust
Partner, Washington
+1 202 662 5329
RQuillian@cov.com



Carolyn Rashby
Employment
Of Counsel, San Francisco
+1 415 591 7095
CRashby@cov.com



Christen Sewell
Employee Benefits and
Executive Compensation
Partner, Los Angeles
+1 424 332 4772
CSewell@cov.com



Lauren Zehmer
Antitrust / Competition
Partner, Washington
+1 202 662 5906
LZehmer@cov.com



Jenna Wallace
Employee Benefits and
Executive Compensation
Of Counsel, New York
+1 212 841 1093
JWallace@cov.com

Treasury Department Moves to Enhance CFIUS's Enforcement Authorities

Executive Summary

On April 11, 2024, the Department of the Treasury, as Chair of the Committee on Foreign Investment in the United States (“CFIUS”), issued a Notice of Proposed Rulemaking (“NPRM”) entitled *Amendments to Penalty Provision, Provision of Information, Negotiation of Mitigation Agreements, and Other Procedures Pertaining to Certain Investments in the United States by Foreign Persons and Certain Transactions by Foreign Persons Involving Real Estate in the United States*.^[1] The NPRM proposes revisions to CFIUS’s existing authorities in the context of non-notified transactions, mitigation agreement negotiations, and the imposition of civil monetary penalties.

- 1 Background—How did we get here?**
- 2 Key Elements of the NPRM**
- 3 CFIUS’s Authority to Request Information and Require Responses**
- 4 Timeframe for Responding to Proposed Mitigation Terms**
- 5 Civil Monetary Penalties**



1 Background—How did we get here?

Parts 800 and 802 of Title 31 of the Code of Federal Regulations implement the provisions of section 721 of the Defense Production Act, as amended, 50 U.S.C. § 4565 (“Section 721”). Part 800 deals with “covered transactions,” while Part 802 deals with “covered real estate transactions.” Among many other things, Parts 800 and 802 provide authority for CFIUS to issue questions and requests for information to parties in various circumstances. Parts 800 and 802 also authorize CFIUS to negotiate and enter into mitigation agreements with parties to covered transactions or covered real estate transactions in order to mitigate risks to U.S. national security that arise as a result of those transactions. Further, Parts 800 and 802 authorize CFIUS to impose civil monetary penalties for violations of Section 721, Parts 800 and 802, or mitigation agreements or conditions.

The NPRM proposes amendments to these authorities to address what the Treasury Department perceives to be gaps in CFIUS’s existing powers. Specifically, the amendments aim to (1) expand CFIUS’s authority to request (and require) information from parties, including outside the context of a transaction that is under review by the Committee; (2) require parties who are negotiating mitigation terms with CFIUS to “substantively respond” to mitigation proposals within three business days; and (3) expand CFIUS’s authority to issue larger civil monetary penalties in more contexts for violations of Parts 800 and 802 or mitigation agreements with CFIUS.

2 Key Elements of the NPRM

As noted above, the updates to Parts 800 and 802 broadly fall into three categories. We set forth each category below and discuss potential impacts (and in some cases, the lack of meaningful practical impact) that the updates may have.

3 CFIUS’s Authority to Request Information and Require Responses

Under Section 721 and Parts 800 and 802, CFIUS is authorized to identify covered transactions and covered real estate transactions that have not been notified or declared to the Committee (commonly referred to as “non-notified transactions”).

[2] The current regulations also address parties’ obligations to respond to those inquiries and certain requests for information.

[3] The NPRM proposes to expand these authorities by expressly authorizing CFIUS to request information in order to determine

if a non-notified transaction may have triggered the mandatory filing requirement as well as whether the transaction may implicate national security considerations.

The NPRM proposes additional amendments that address two other circumstances. First, the amendments would require parties to provide information to CFIUS when CFIUS seeks information to monitor compliance with or enforce the terms of an existing mitigation agreement, order, or condition. Second, the amendments would require parties to provide information to CFIUS when it seeks that information to determine whether transaction parties have made a material misstatement or omitted material information during the course of a previously concluded review or investigation (including in circumstances where the review ended with CFIUS rejecting the parties’ notice).

Notably, each of the foregoing largely reflects CFIUS’s existing practices. For example, in practice CFIUS already asks questions to ascertain whether filings may have been mandatory or whether the non-notified transaction may implicate U.S. national security considerations. We believe it is likely that these formalizing updates to the Committee’s authorities are a result of a relatively small number of edge cases where parties have declined to respond to questions from CFIUS regarding a non-notified transaction on the basis that the questions did not strictly relate to ascertaining CFIUS’s jurisdiction. These revisions would close that perceived gap.

We do not anticipate that those revisions will meaningfully impact the Committee’s internal decision-making about those non-notified transactions for which it ultimately requests a filing from the parties. While the NPRM suggests that these revisions will “allow the Committee to prioritize transactions that parties were required to submit . . . or that, in its view, otherwise warrant formal review,” this is consistent with existing practice. CFIUS has finite resources to review transactions, including non-notified transactions, and it is already more likely to request a filing for a non-notified transaction about which it has substantive concerns, either because it suspects a filing was mandatory for the transaction or because it views the transaction as implicating U.S. national security interests.

Similarly, the amendments requiring parties to respond to CFIUS’s inquiries in the context of monitoring compliance with existing mitigation arrangements or previously concluded reviews or investigations appear merely to formalize what is already a common practice. While it may be possible in some circumstances for parties to decline to respond to CFIUS’s inquiries in those types of circumstances, parties do so at their own peril.

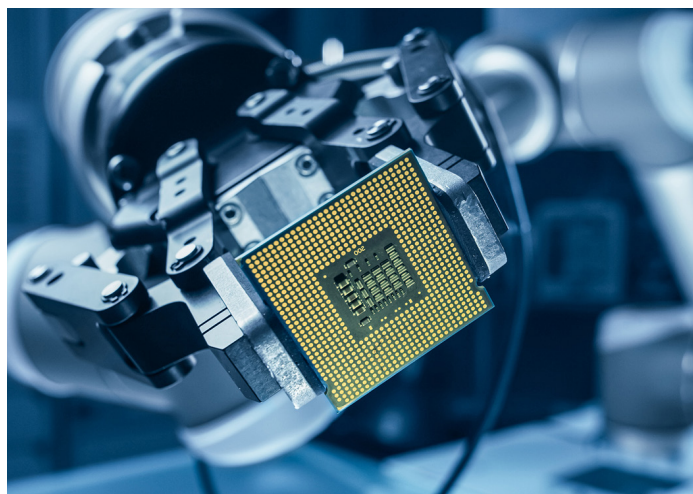
Thus, for the most part, the foregoing amendments simply clarify and make explicit how CFIUS has operated in pursuing information, and we do not see them as effecting any material change for transaction parties and their approach to CFIUS.

The NPRM also proposes expanding CFIUS’s subpoena power by revising the current language of the regulations—which states that CFIUS can issue subpoenas “[i]f deemed *necessary* by the Committee”^[4]—to allow CFIUS to issue a subpoena when deemed *appropriate* by the Committee. This proposed change is interesting because it raises the question of whether CFIUS intends to alter its existing practice of seeking information through more informal requests (which nevertheless produce responses) to issuing subpoenas, which other regulators, such as the Securities and Exchange Commission, regularly use to elicit information. We do not believe that necessarily is Treasury’s intent; rather, we think that this proposal is intended to make it easier for CFIUS to ratchet up a request by issuing a subpoena in the rare circumstance that parties have not provided sufficient information on a voluntary basis. But if the change in practice were more dramatic—i.e., if CFIUS moved from seeking information through written requests to routinely issuing subpoenas to compel responses—it indeed would be a notable change, and position CFIUS in a more adversarial posture vis-à-vis transaction parties.

4 Timeframe for Responding to Proposed Mitigation Terms

The current regulations at Parts 800 and 802 do not provide a specific timeline for parties to respond to proposed mitigation terms from CFIUS. In contrast, the regulations do require transaction parties to respond to information requests by the Committee in connection with a notice or declaration within three or two business days of the request, respectively.^[5] The NPRM proposes to implement an analogous timeline for parties to respond to mitigation proposals from the Committee—transaction parties would be obligated to “substantively respond”^[6] to mitigation proposals within three business days. If the transaction parties fail to do so, CFIUS could reject the notice under review. The revisions also provide for extensions in certain circumstances, including (but not limited to) initial mitigation proposals and circumstances where the proposed mitigation is complex, and the parties require more than three business days to review it. The NPRM further states that CFIUS may grant “reasonable extension requests,” taking into account factors such as the remaining time on the statutory review clock and whether the transaction under review was filed before closing.^[7]

The stated reason for these revisions is that the absence of an express time limit “can sometimes result in a protracted process where parties take longer than is reasonable to



respond to the Committee’s proposed terms.”^[8] The NPRM notes that these delays by parties “impede the Committee’s ability to fulfill its statutory obligation to complete an investigation in 45 days” and can result in the withdrawal and refiling of the notice by the parties in order to facilitate further negotiation on mitigation terms.^[9]

To put it plainly, this is a classic example of the pot calling the kettle black. Transaction parties—disciplined by market forces and the often-substantial costs associated with regulatory delays of any kind—nearly always are focused on timing and bringing transactions to a close within the statutory timeline. *In fact, it is the transaction parties themselves who are routinely kept waiting for the Committee, as a result of its own processes, to propose mitigation terms or to respond to draft mitigation agreements.* While we cannot cite empirical data, we can cite our own long experience that the government takes longer—often much longer—than the transaction parties to respond to draft mitigation terms. Indeed, there have been many cases over the years that have lasted longer—and required withdrawals and refilings—owing to Committee dynamics rather than delay by the parties. In those instances in which the Committee waits longer on transaction parties, it is typically because the proposed mitigation terms create substantial transactional or business impacts, or even constructively—if unintentionally—have the effect of prohibiting a transaction given the crippling commercial impact of the proposed terms. As we have advised clients for decades, the government excels at diagnosing the ailments within a transaction (i.e., the national security impact); on the other hand, it is not nearly as adept at prescribing solutions that are workable for businesses. This is neither new nor an inherent obstacle—it is a natural aspect of the negotiation of CFIUS mitigation terms for the government and transaction parties to have to iterate to identify the right formulation that protects the government’s

interests while also being commercially feasible.

We note that it was not always the case that parties were waiting on the government to respond to draft mitigation terms, or that the government's inter-agency processes delayed engagement on mitigation terms. Many years ago, parties could engage early and energetically in the review process with the key CFIUS agencies and work together on mitigation terms even before the co-lead agencies had finalized their risk-based assessment. This practice, while efficient, became disfavored out of a concern that it resulted in individual agencies effectively running their own CFIUS processes, contributing to circumstances of over-mitigation. There is, therefore, some benefit to the Committee's more formal rules, which require co-lead agencies for a particular matter to adhere closely to a formal risk-based assessment that is evaluated by the full Committee. In theory, this more formalized process *should* result in the Committee being more disciplined and mitigation terms being better calibrated—which should inure, overall, to the benefit of transaction parties. Having negotiated mitigation agreements for several decades, however, it is our view that the Committee has over-indexed on internal government process, with the effect of delaying negotiation of mitigation agreements and resolving matters less expeditiously.

In sum, sophisticated transaction parties who are repeat players with CFIUS will rightly be incredulous at the notion that the delays in mitigation are more attributable to the parties than to the government. These parties will recognize that imposing a three-day requirement to respond to mitigation is not a cause of concern (because they generally will want to bring CFIUS to a close sooner than later), and, at the same time, will accomplish nothing in terms of expediting the process as long as the dynamics described above remain unchanged. What would be more likely to have a salutary impact on timing—as well as to build confidence and relationships that will help with monitoring agreements once they become effective—is to restore more of an equilibrium between the formality of the Committee's process and the prior art of direct engagement with transaction parties on potential solutions to the government's concerns. And if CFIUS really wishes to instill confidence in the mitigation process, it would impose a concomitant deadline *on the government* to respond to successive turns of a mitigation agreement by the transaction parties.

5 Civil Monetary Penalties

Parts 800 and 802 set forth the amounts for civil monetary penalties that the Committee may impose for various situations, including (1) the submission of a declaration or notice with a material misstatement or omission, or the making of a false certification;^[10] (2) the failure to comply

with the requirements for mandatory CFIUS filings;^[11] and (3) violations of orders issued by the Committee, material provisions of mitigation agreements, or material conditions imposed by the Committee.^[12]

The NPRM proposes significant modifications to these provisions. Specifically, the proposed revisions would increase the amount of potential civil monetary penalties under the three scenarios above as follows:

- the maximum penalty under situation (1) above would increase from \$250,000 to \$5,000,000 (per violation);
- the maximum penalty under situation (2) above would increase from the greater of \$250,000 or the value of the transaction (per violation) to the greater of \$5,000,000 or the value of the transaction (per violation); and
- the maximum penalty under situation (3) above would increase from the greater of \$250,000 or the value of the transaction (per violation) to the greater of \$5,000,000, the value of the transaction, or the value of the party's interest in the U.S. business at the time of the violation or the time of the transaction (per violation).

Additionally, the revisions would expand CFIUS's authority to issue civil monetary penalties for material misstatements and omissions to additional contexts outside of declarations and notices. The Committee would have authority to issue such penalties to material misstatements and omissions in connection to requests for information related to non-notified transactions, responses to certain information requests from CFIUS in the context of monitoring or enforcing compliance with mitigation terms, and also for information requests from the Committee in other contexts such as agency notices.

Finally, the revisions would update the timeline for parties to submit a petition for reconsideration of a penalty by the Committee. Under the proposal, the parties would have 20 business days to submit such a petition, and the Committee would have 20 business days to assess the petition and issue a final penalty determination.

These are major changes to CFIUS's penalty powers. The NPRM explains that CFIUS has determined that the \$250,000 limit under existing regulations—which it notes is not specified by Section 721 and was put in place over 15 years ago—does not create sufficient deterrent effect in certain contexts. For example, the NPRM notes that under the broad definition of "transaction," certain transactions may have a low value (or in some cases, a valuation of zero dollars). In that situation, CFIUS could only impose \$250,000 per violation, which may not be—in the Committee's view—sufficiently punitive to deter violations. (Though we note, as does the NPRM, that criminal penalties may attach under 18 U.S.C. § 1001 to making false statements to the government.)



We see this focus on increasing monetary penalties to incentivize compliance as misplaced. We have yet to experience a matter where the size of the potential civil money penalty would likely have had any impact on the particular compliance weakness; such weaknesses or issues most typically arise not because parties are actively seeking to avoid their obligations under a mitigation agreement but rather due to such factors as human error or misunderstandings as to the meaning of mitigation terms that often have been negotiated in great haste. To the extent that there are weaknesses, it more often relates to other organizational controls or the capabilities of security officers (i.e., the individuals charged with day-to-day compliance of the mitigation agreements). Moreover, one significant historical challenge has been the unevenness of the government's approach to monitoring and compliance, with the result that the substantive focus on any given mitigation agreement could vary from year to year, agency to agency, or even among successive officials from the same agency. Another challenge that remains is ensuring consistency in understanding and analysis in the "hand-off" between the teams within agencies who negotiate the mitigation terms and the teams responsible for monitoring compliance. To the credit of the current leadership of CFIUS, we have seen meaningful improvement on these fronts over the last 12 to 24 months, though there is still more room for maturity and consistency—especially consistency in the agencies' understanding of terms as negotiated and how those same terms are implemented and monitored.

Considering this history, we respectfully suggest that the government is more likely to incentivize enhanced compliance

by engaging more collaboratively during the mitigation negotiations, continuing its efforts to mature its monitoring framework, and setting clear expectations as part of its oversight responsibilities.

[1] The NPRM is scheduled to be published in the Federal Register on April 15, 2024.

[2] See 31 C.F.R. 800.501(b) and 802.501(b).

[3] See *id.* at 800.801(a) and 802.801(a).

[4] See *id.*

[5] See *id.* at 800.406(3); 800.504(4); 802.404(3); 802.504(4).

[6] The NPRM states that the Committee expects a "substantive response" "to consist of acceptance of the terms, a counterproposal, or a detailed statement of reasons that the party or parties cannot comply with the proposed terms, which may also include a counterproposal." NPRM at 9.

[7] See *id.* at 9-10.

[8] See *id.* at 9 (emphasis added).

[9] See *id.*

[10] 31 C.F.R. 800.901(a); 802.901(a).

[11] See *id.* at 800.901(b). Note that there is no counterpart provision for mandatory declarations in part 802 with respect to real estate transactions.

[12] See *id.* at 800.901(c); 802.901(b).

**David Fagan**

Regulatory and Public Policy / CFIUS
Partner, Washington
+1 202 662 5291
DFagan@cov.com

**Heather Finstuen**

Regulatory and Public Policy / CFIUS
Partner, Washington
+1 202 662 5823
HFinstuen@cov.com

**Mark Plotkin**

Regulatory and Public Policy / CFIUS
Partner, Washington
+1 202 662 5656
MPlotkin@cov.com

**Jonathan Wakely**

Regulatory and Public Policy / CFIUS
Partner, Washington
+1 202 662 5387
JWakely@cov.com

**Ingrid Price**

Regulatory and Public Policy / CFIUS
Special Counsel, Washington
+1 202 662 5838
IPrice@cov.com

**Janine Slade**

Regulatory and Public Policy / CFIUS
Special Counsel, Washington
+1 202 662 5239
JSlade@cov.com

**Brian Williams**

Regulatory and Public Policy / CFIUS
Senior Advisor, Washington
+1 202 662 5270
BWilliams@cov.com

**Lawrence Barker**

Regulatory and Public Policy / CFIUS
Associate, Washington
+1 202 662 5437
LBarker@cov.com

**Ian Carrico**

Regulatory and Public Policy / CFIUS
Associate, Washington
+1 202 662 5238
ICarrico@cov.com

**Jacob Crump**

Regulatory and Public Policy / CFIUS
Associate, Washington
+1 202 662 5591
JCrump@cov.com

**Irina Danescu**

Regulatory and Public Policy / CFIUS
Associate, Washington
+1 202 662 5556
IDanescu@cov.com

**Samuel Karson**

Regulatory and Public Policy / CFIUS
Associate, Washington
+1 202 662 5341
SKarson@cov.com

**Fiza Khan**

Regulatory and Public Policy / CFIUS
Associate, Washington
+1 202 662 5690
FKhan@cov.com

**Brian Kim**

Regulatory and Public Policy / CFIUS
Associate, Washington
+1 202 662 5703
BKim@cov.com

**Monty Roberson**

Regulatory and Public Policy / CFIUS
Associate, Washington
+1 202 662 5903
MRoberson@cov.com

**Madeline Sanderford**

Regulatory and Public Policy / CFIUS
Associate, Washington
+1 202 662 5408
MSanderford@cov.com

Two Updates Published by the UK FCA on the Anti-Greenwashing Rule, and the SDR and Labelling Regime

On 23 April 2024, the FCA released two important publications relating to its Sustainability Disclosure Requirements (“SDR”) and investment labelling regime:

- 1. Relevant to all FCA-authorized firms:** the FCA’s [finalised guidance](#) (FG 24/3) on the anti-greenwashing rule, with both the rule and finalised guidance coming into force on 31 May 2024; and
- 2. Relevant to firms providing portfolio management services:** a [consultation paper](#) (CP 24/8) setting out the FCA’s proposal to extend the SDR and investment labelling regime that will be applicable to asset management firms from 31 May 2024, to all forms of portfolio management services. As the SDR and labelling regime are developed principally for the benefit of retail investors, the proposed extension is aimed at wealth management services for individuals and model portfolios for retail investors, though firms offering portfolio management services to professional clients can opt into the labelling regime.

The FCA’s finalised non-handbook guidance on the anti-greenwashing rule

What is the anti-greenwashing rule?

The FCA has emphasised that tackling greenwashing – where firms make exaggerated, misleading and/or unsubstantiated sustainability claims regarding their products or services – is a regulatory priority. From 31 May 2024, ESG 4.3.1R – ‘the anti-greenwashing rule’ - will apply to client communications and financial promotions of all FCA-authorized firms - providing that when a claim is made regarding a financial product or service’s sustainability characteristics (a concept which is defined to capture both environmental and social characteristics), the firm will be responsible for ensuring that this claim is:

- a. accurate; and
- b. fair, clear and not misleading.



Why is the non-handbook guidance important?

The non-handbook guidance is intended to help firms gain a better understanding of the FCA's expectations regarding the application of the anti-greenwashing rule, with (non-exhaustive) practical examples included throughout. Firms (including those firms applying for authorisation from the FCA) should therefore review the guidance to ensure their understanding of the FCA's expectations of the rule, and consider the changes to be built into their client communications and financial promotions frameworks and the related monitoring processes.

The guidance clarifies that:

1. The anti-greenwashing rule is intended to complement and be consistent with: (i) other FCA 'fair, clear and not misleading' requirements; (ii) the Consumer Duty's consumer understanding outcome rules under PRIN 2A.5; and (iii) the ASA requirements and CMA guidance relating to environmental claims.
2. While the scope of the anti-greenwashing rule relates to **products and services**, firms are reminded that the CMA and ASA Guidance, FCA Principles 6 and 7, or (as relevant) the Consumer Duty (Principle 12 and PRIN 2A), apply to sustainability-related claims **that a firm may make about itself as a firm**.
3. Further, firms should take into account **how firm-level claims may be considered as part of the 'representative picture' in a decision-making process**.
4. Sustainability claims should:
 - be factually correct and capable of being substantiated with robust and credible evidence, for as long as the claim is being communicated (i.e. however long the financial promotion is live);
 - be clear and presented in a way that can be understood by the intended audience –for firms subject to the Consumer Duty, this will mean testing that communications are likely to be understood by customers and that they meet customers' information needs in a way that enables them to make effective, timely and properly informed decisions;
 - be complete, such that they do not omit or hide important information, but rather provide a representative picture of the product or service and its full life-cycle; and
 - only include comparisons to other products or services (including previous versions of the firm's own products or services) where such comparisons are fair and meaningful.
5. Where firms rely on third parties for information, they should consider whether it is appropriate to rely on such data, research or analytical sources to substantiate the claims being made.

Our thoughts

The finalised guidance serves as a helpful practical resource for firms - with numerous 'real-life' illustrative examples added following feedback received on its draft guidance, as well as further commentary on the scope of the rule and how it interacts with other FCA rules.

The significance of Points 2 and 3 above should not be underestimated – not least, in the current environment in which firms feel increasingly compelled to 'showcase' their own virtues (including sustainability credentials). The FCA's view that firm-related claims may be considered as part of the 'representative picture' in a decision-making process is a particularly noteworthy warning signal on which firms would be well-advised to reflect.

The proposed extension of the SDR and labelling regime to portfolio management firms

What is the FCA proposing?

In response to its initial 2022 consultation (CP 22/20) on the then-proposed SDR and labelling regime, the FCA received feedback relating specifically to the application of the regime to portfolio management firms. As a result of this feedback, the FCA is now proposing to extend the SDR and labelling regime to portfolio management services, as summarised below. "Portfolio management" in this context is defined as a service provided to a client which comprises either: (a) managing investments; or (b) private equity or other private market activities consisting of either advising on investments or managing investments on a recurring or ongoing basis in connection with an arrangement, the predominant purpose of which is investment in unlisted securities.

The FCA proposes to extend the SDR and investment labels regime to all forms of portfolio management services, including where the portfolio management offering (the agreements or arrangements) are model portfolios, customised portfolios and/or bespoke portfolio management services (tailored to the clients' needs and preferences).

- **Labels:** In addition to meeting the other qualifying criteria under ESG 4.2.4R, portfolio management offerings will be able to use a sustainability label if 70% or more of the gross value of the assets within the portfolio are invested according to the sustainability objective.
- **Naming and marketing rules:** All portfolio management offerings to retail investors will be subject to the naming and marketing rules under ESG 4.3.

- **Consumer-facing disclosures:** Production of consumer-facing disclosures (with the information required under ESG 5.2) when the firm uses a label or sustainability-related terms without a label.
- **Product-level disclosures:** Production of pre-contractual disclosures and ongoing product-level disclosures when using a label or sustainability-related term without a label.
- **Entity-level disclosures:** Firms with over GBP 5 billion in AUM will need to produce entity-level disclosures in relation to the overall assets managed in relation to the relevant business.
- **Distributor rules:** Distributors will need to provide labels and consumer-facing disclosures to retail investors.

What is the timeline for implementation?

The FCA is accepting feedback to its consultation until 14 June 2024. Following this, it intends to publish the final rules in the second half of 2024, with the following suggested implementation timeline:

RULES	PROPOSED IMPLEMENTATION DATE
Labelling, naming and marketing requirements and the associated consumer-facing and pre-contractual disclosures	2 December 2024
Ongoing product-level disclosures	2 December 2025*
Entity-level disclosures	<i>For firms with AUM over GBP 50 billion: 2 December 2025*</i>
	<i>For firms with AUM over GBP 5 billion: 2 December 2026*</i>

* Consistent with the dates on which the rules will be in force for fund managers.



David Berman
Financial Services
Partner, London
+44 20 7067 2190
DBerman@cov.com



Emily Lemaire
Financial Services
Associate, London
+44 20 7067 2291
ELemaire@cov.com

COVINGTON

BEIJING BOSTON BRUSSELS DUBAI FRANKFURT JOHANNESBURG LONDON
LOS ANGELES NEW YORK PALO ALTO SAN FRANCISCO SEOUL SHANGHAI WASHINGTON

www.cov.com

© 2024 Covington & Burling LLP. All rights reserved.