



HUNTON
ANDREWS KURTH

RETAIL INDUSTRY

//////
2022 YEAR IN REVIEW

Published in January 2023



Dear Clients and Friends,

2022 was another remarkable year for the retail industry. We continue to partner with our retail clients through these extraordinary times, striving to provide top-notch, innovative legal solutions and insight.

Our retail team of more than 300 lawyers is recognized by *Chambers USA* as one of the top retail groups in the country, highlighting our deep understanding of issues facing the retail industry and our exceptional client service. We advise more than 500 retail and consumer products clients across a wide range of complex transactional, litigation and regulatory matters in the United States and abroad. Our lawyers are actively involved with organizations that support the retail industry, allowing us to work closely with industry leaders to identify emerging trends and matters of critical importance. We have achieved significant results for an impressive list of household name clients, and we are well-positioned to support our clients' key initiatives as they confront fierce competition in an evolving global marketplace.

What type of retail innovation or complication do you expect to face in the coming year: Artificial intelligence or other emerging technologies? Sustainability concerns? Fraud and loss prevention challenges? Our lawyers remain on the forefront of both traditional and disruptive issues that matter most to our retail clients. Whether you need brick-and-mortar, e-commerce, or metaverse related counsel, we are here and ready to assist.

Our *2022 Retail Industry Year in Review* provides a comprehensive overview of recent developments impacting retailers, as well as a look ahead at what to expect in 2023. This year's publication highlights key topics such as cyber insurance, M&A activity, regulation and litigation related to PFAS, labor organizing, developments in ESG disclosure, and many others.

I hope that our *2022 Retail Industry Year in Review* will be a valuable resource full of useful commentary and analysis on the issues that are essential to you and your company. We look forward to serving our retail clients in 2023 and beyond.


Wally Martinez
Managing Partner

The American Lawyer Named
Hunton Andrews Kurth's California
Litigation Team Among Finalists
for Regional Litigation
Department of the Year

TABLE OF CONTENTS

Do the Products You Sell Contain PFAS? A Question Every Retailer Must Be Prepared to Answer	6
Looking Into the Merger Review Crystal Ball: New Trends That Will Shape Future Enforcement	11
Sellers Beware: Recent String of Court Decisions Pose New Risks for Digital Marketplaces	14
Following on the FTC's Heels, Plaintiffs' Firms File Dozens of Class Actions Against Retailers and Manufacturers Alleging Technical Violations of the Magnuson-Moss Warranty Act	18
2022 Litigation Trends for PFAS-Containing Consumer Products and 2023 Preview	22
Check Your Inventory; Do You Have Enough Cyber Insurance?	26
Accountability in Cybersecurity and Privacy: Keeping Your Name Out of the Headlines	30
2022 Retail M&A Year in Review	36
Getting Hot in Here: Workplace Safety Regulators Address Employee Heat Illnesses	40
Labor Organizing in Retail: 2022 Review	45
2022 Marks a Large Step Forward for ESG Disclosure	49
Key Contacts	58
About Us	59





Do the Products You Sell Contain PFAS? A Question Every Retailer Must Be Prepared to Answer

Per- and polyfluoroalkyl substances (PFAS) have taken center stage. The Biden administration's regulatory agenda plans numerous revisions to environmental regulations to address this broad class of pervasive substances. While the US Environmental Protection Agency grapples with implementing these initiatives, states are aggressively forging ahead with their own plans. Laws targeting PFAS in various products have taken effect and will continue to take effect in many states, representing a striking expansion from typical state regulations addressing environmental PFAS contamination from firefighting foam and other sources. To manage liability, retailers must be aware of this trend and understand the expanding regulatory requirements and potential liability for selling products containing PFAS in states with these restrictions.



State Regulation of PFAS in Products

Previously, states targeted chemicals such as BPA, phthalates, lead, cadmium and flame retardants in consumer products. However, given the significant public interests in addressing PFAS, states are turning their focus to this class of chemicals. The approximately [280 PFAS-related bills](#) proposed by states in 2022 demonstrate the states' prioritization of PFAS regulation.

Until recently, only states with existing chemical regulatory programs sought to restrict PFAS in products. For example, California's Department of Toxic Substances Control designated rugs, carpets and converted textile/leather treatments containing PFAS as "priority products" for which the state's Safer Consumer Products Program mandates disclosures from responsible entities and could require alternative analyses and future bans. Children's products laws in New York and Vermont authorize regulators to require perfluorooctanoic acid (PFOA) and perfluorooctane sulfonic acid (PFOS) reporting in children's products, while Oregon and Maine require similar reporting for just PFOS. California's Proposition 65 already requires warnings for products sold in California containing certain PFAS above safe harbor levels.

To date, 11 states have enacted laws banning PFAS as a class in products ranging from children's products, textiles, cosmetics, furniture, food packaging, rugs, carpets, fabric treatments and ski wax. Maine's law proved the most sweeping, covering all consumer products sold in the state. States' deadlines are outlined below:

State Bans on PFAS in Products¹

State	Products Regulated	Compliance Date
California	Food packaging	January 1, 2023
	Juvenile products	July 1, 2023
	Cosmetics ²	January 1, 2025
	Textile articles	January 1, 2025
Colorado	Juvenile products	January 1, 2024
	Carpets and rugs	January 1, 2024
	Oil and gas products	January 1, 2024
	Fabric treatments	January 1, 2024
	Food packaging	January 1, 2024
	Indoor upholstered furniture	January 1, 2025
	Cosmetics	January 1, 2025
	Indoor textile furnishings	January 1, 2025
	Outdoor upholstered furniture	January 1, 2027
Outdoor textile furnishings	January 1, 2027	
Connecticut	Food packaging	As soon as feasible but no later than December 31, 2023
Hawaii	Food packaging	July 1, 2023
Maine	Carpets, rugs and fabric treatments	January 1, 2023
	All consumer products	January 1, 2030
	Pesticides	January 1, 2030
Maryland	Food packaging	January 1, 2024
	Rugs and carpets	January 1, 2024
	Cosmetics ³	January 1, 2025
Minnesota	Food packaging	January 1, 2024
New York	Food packaging	December 31, 2022
	Apparel	December 31, 2023
Rhode Island	Food packaging	January 1, 2024
Vermont	Rugs, carpets	July 1, 2023
	Food packaging	July 1, 2023
	Ski wax	July 1, 2023
	Aftermarket stain and water-resistant treatments	July 1, 2023
Washington	Food packaging	February 2023 and May 2024 ⁴

¹ This table omits state disclosure or labeling laws.

² Applies only to certain PFAS.

³ Applies only to certain PFAS.

⁴ The Washington statute authorizes its state agency to ban PFAS in food packaging two years after issuing an alternatives analysis. The agency has released two alternatives analyses. PFAS in food packaging products discussed in the first report are prohibited as of February 2023, and PFAS in the products discussed in the second report are prohibited as of May 2024. For more information visit: <https://ecology.wa.gov/About-us/Who-we-are/News/2022/May-19-State-takes-steps-toward-banning-PFAS-in-fo>.



“I have found the attorneys at Hunton Andrews Kurth to be very proactive, creative and curious - the service and responsiveness has been excellent.”

Chambers USA

“Across the board they’ve got incredibly good attorneys. I’m continually impressed by how practical they are.”

Chambers USA

Supply Chain Challenges and How Retailers Can Prepare

The number of PFAS product bans will continue to grow annually. One significant challenge facing manufacturers, importers, distributors and retailers is states' broad definition of PFAS—"a class of fluorinated organic chemicals containing at least one fully fluorinated carbon atom"—that would sweep potentially thousands of chemicals under PFAS regulations. And, notably, these laws prohibit any amount of intentionally added PFAS in products and, in some instances, certain percent concentrations of PFAS whether intentionally added or not. To comply, companies need to understand not only their products' components, but also their chemical composition at the molecular level. Adding to this complexity is the states' varied patchwork of regulated products subject to differing dates of implementation, as evidenced by the nine different food packaging regulations in the 11 states highlighted in the preceding table.

Stringent compliance demands have forced companies to choose between expensive independent testing or reliance on supplier representations about PFAS presence in products. For retailers specifically, many state PFAS laws make "any person" strictly liable for selling violative products in the state, regardless of knowledge or responsibility for introducing PFAS into the products.

To prepare for future challenges, retailers should consider implementing the following steps:

- Begin communicating with suppliers early to ensure they are aware of any PFAS-related products bans and ask them to provide assurances/certifications that their products comply with state laws. In these certifications, retailers should be careful to define PFAS appropriately in accordance with state laws and understand the thresholds for compliance, whether it be any intentionally added PFAS or if the laws include any PFAS byproducts or impurities.
- Incorporate indemnity language in supplier agreements to pass liability to the manufacturer or distributor of the product in the event of noncompliance liability.
- Be aware of the state laws that offer relief for retailers in the event they received certificates of compliance from manufacturers, and ensure that those certificates meet all requisite criteria to qualify for such relief.
- Continue to track PFAS legislation, regulation and enforcement trends in states where they operate retail stores or sell products. This may be particularly challenging for online retailers with limited knowledge or control over where their products end up in commerce.

For more information about PFAS product regulations, please contact Hunton Andrews Kurth's PFAS interdisciplinary team.

Looking Into the Merger Review Crystal Ball: New Trends That Will Shape Future Enforcement

Merger review at the federal antitrust agencies took a turn in 2022, as new leadership at the Federal Trade Commission (FTC) and Department of Justice (DOJ) began to hit their stride and implement new enforcement priorities. The pace of merger challenges picked up—as compared to the first year of the Biden administration—and the issues taken on by the agencies have developed according to announced policy changes that will likely shift the focus of the analytical approach applied in evaluating the legality of mergers in coming years. For retailers, these trends mean that future M&A activity may require consideration of additional issues that are now cropping up within the scope of merger investigations.

Retailers considering mergers should be aware of the agencies' current scrutiny of noncompetes entered into in connection with the sale of a business, as well as the increased focus on upstream markets such as labor markets.

Noncompetes have received increased attention since President Biden's 2021 Executive Order on Competition encouraged the FTC to "curtail the unfair use of non-compete clauses and other clauses or agreements that may unfairly limit worker mobility." And while the spotlight on noncompetes has largely been in the context of employer/employee noncompete agreements, M&A noncompetes have also drawn scrutiny. In June 2022, the FTC took action against a completed, non-Hart-Scott-Rodino (HSR) reportable transaction by ARKO to acquire 60 gas stations wherein the parties had agreed to a lengthy noncompete covering more than 190 locations where the buyer had existing operations. The FTC alleged the noncompete provision in the purchase agreement as overly broad, and sought to limit its terms to three years and three miles from the acquired locations only, and further to invalidate all similarly overbroad noncompetes in favor of the buyer arising out of any other previous transaction. The FTC's



Javaneh Tarter, Gregory Wall, Matthew Leopold, Malcolm Weiss, Nancy Beck, PhD, Paul Nyffeler, PhD

Javaneh is a senior attorney, Greg is a partner, Matt is a partner, Malcolm is a partner, Nancy is Director of Regulatory Science and Paul is a senior attorney on the environmental team in various firm offices.

Recognized in
Benchmark Litigation's
2023 guide to the
USA's leading litigation
firms and lawyers

analysis proclaimed “[n]oncompete agreements affecting areas geographically distinct from acquired [businesses], and noncompete agreements untethered to protecting goodwill acquired in the acquisition, are highly suspect and warrant Commission scrutiny.” In a statement released with the complaint, FTC Chair Lina Khan noted that enhanced scrutiny of noncompetes would be applied to business sales and mergers, particularly where the two parties are “actual and potential rivals” who will “remain competitors in other markets” after the transaction.

Consideration of competition for labor as an input is not entirely new, but the anticipated revision of the Merger Guidelines—as presaged by a January 2022 request for information seeking public comments about merger enforcement policy—highlights the agencies’ likely expanded focus on questions about the impact of mergers on labor markets. In October 2022, the DOJ successfully challenged the \$2.2 billion proposed merger between Penguin Random House and Simon & Schuster. The companies subsequently abandoned the deal. The case was notable for the DOJ’s focus on harm to an upstream market, namely authors selling the rights to publish their works, rather than downstream consumers as the ultimate buyers of books. The court found that the deal would reduce competition between publishers vying to purchase the rights to the most well-known authors and would harm competition in the market for publishing rights to anticipated top-selling books. The DOJ’s victory will likely give the agencies the momentum they need to continue pursuing similar legal theories in future cases.

The past year also saw a change in the FTC’s approach to settling merger cases as it revived its use of prior approval provisions. The DOJ has not appeared to follow this approach thus far.

Prior approval provisions require parties to notify the agency of future transactions—even when those transactions fall below HSR filing thresholds—and shift the burden of proof to the parties to establish that the future transactions are not anticompetitive, flipping the burden that the agency normally bears. In 2021, the FTC rescinded a 1995 policy statement on prior notice and prior approval that limited the circumstances in which these provisions would be imposed, and adopted

a new policy statement that announces the FTC will “routinely require merging parties subject to a Commission order to obtain prior approval from the FTC before closing any future transaction affecting each relevant market for which a violation was alleged.” These prior approval provisions will cover deal activity of the merging parties for a minimum of 10 years, including requiring buyers of divested assets “to agree to a prior approval for any future sale of the assets they acquire in divestiture orders.” The shift to prior approval was front and center in June 2022, clearing the way for a \$1.1 billion merger of veterinary clinics through a settlement wherein the buyer JAB committed to getting prior approval of any acquisition within 25 miles of a JAB veterinary clinic anywhere in California or Texas. Whereas advocates of the new prior approval policy claim that it provides the FTC with an opportunity to investigate potentially unreportable transactions before they are consummated, critics suggest that it encourages parties to adopt a “fix-it-first” approach to transactions—whereby overlapping assets are disposed prior to agency review—in order to avoid subjecting mergers to the prior approval process, with the ultimate result being less FTC oversight and input into the proper structural remedies to preserve competition following mergers.

Finally, for merger challenges that do get litigated, courts are currently grappling with the issue of deciding which party bears the burden of proving the competitive implications of a proposed divestiture. This topic is suddenly up for debate after a court ruled against the DOJ in its attempt to block UnitedHealth’s acquisition of Change Healthcare, holding that the DOJ had failed to show that the *remedied* merger would substantially lessen competition. Previously, courts reviewing merger challenges had mostly held that if the government was able to show that the *unremedied* merger may substantially lessen competition, then the evidentiary burden would

shift to the defendants to show that the divestiture adequately restored competition. Now, the framework for litigating such merger challenges appears to be an open question, which may give parties greater incentives to fend off overly aggressive agency settlement proposals and instead contest their preferred divestiture package in court. As seen in the recent build-up to the DOJ’s challenge in Assa Abloy/Spectrum Brands and the FTC’s action in Microsoft/Activision Blizzard, merging parties appear to like their chances of prevailing.

These changes to the substance and process of merger review are expected to continue to shape the agencies’ evolving merger enforcement priorities, which will affect how retailers plan and execute their own future M&A strategies.



Kevin Hahm and Bennett Sooy

Kevin is a partner and Bennett is an associate in the antitrust and consumer protection practice in the firm's Washington, DC office.

Sellers Beware: Recent String of Court Decisions Pose New Risks for Digital Marketplaces

Introduction

As digital commerce becomes an increasingly ubiquitous aspect of the modern retail economy, the law governing product liability is undergoing a rapid and incongruous evolution. In traditional product liability law, any entity in the product chain, from manufacturer to retailer, is generally subject to strict liability for a defective product. This legal concept has generally been carried over to traditional retailer-hosted website sales, where the retailer directly sells products and collects payment through an online platform. Digital marketplaces, like Amazon Marketplace or eBay, where third parties can directly advertise their products to consumers and collect payment through a hosted website without endorsement (and indeed, often affirmative disclaimer) of the website owner are a relatively new phenomenon. Until recently,

courts had distinguished digital marketplaces from traditional retailers and held that their hosts were not strictly liable for defective products sold by third parties on their platforms. A string of recent court decisions, however, is heading in the other direction, holding the owners of digital marketplaces liable in the same way as a traditional seller. Importantly, these decisions are extending liability not just to instances where the digital marketplace physically controls the product, but to essentially any transaction where the digital marketplace acts as an active intermediary between seller and buyer. If this trend continues, it has the potential to dramatically alter the product liability landscape for digital marketplaces, and it should be on the radar of every online retailer.

Bolger Finds Liability When a Digital Marketplace Controls the Product

The consensus on digital marketplace liability for third-party products was first challenged in *Bolger v. Amazon.com, LLC*.¹ In *Bolger*, a customer purchased a laptop battery on the Amazon marketplace. The battery was not manufactured by Amazon, but was instead sold by a third-party vendor as part of the Fulfilled by Amazon (FBA) program. Under the FBA, Amazon controlled the terms of the sale, collected payment from the customer, charged the vendor a sales fee proportionate to the price of the transaction and shipped the battery from its warehouse in Amazon-branded packaging. Several months later, the battery exploded, severely burning the customer. The customer then sued Amazon, asserting causes of action for strict product liability and negligence. The trial court granted summary judgment for Amazon on the grounds that it did not distribute, manufacture or sell the battery.

The California Court of Appeals reversed the decision, finding that Amazon's control over both the product and the transaction formed a basis for liability. Amazon was not a mere "service provider" or "facilitator" of

the sale, but a "direct link" in the chain of distribution and a "powerful intermediary" between the third-party seller and the consumer. Imposing strict liability afforded "maximum protection" to injured plaintiffs while working no injustice on product sellers, who could allocate "the costs of such protection between them in the course of their continuing business relationship." It was Amazon's choice to offer the product for sale, to store the product at its warehouse, to accept the customer's order and to ship the order. Amazon made these choices for its own "commercial purposes," the court reasoned, and therefore, "should share in the consequences."

Loomis and Sigismondi Expand the Scope of Liability

In April 2021, less than a year after the *Bolger* decision, a second California appellate court considered liability for online marketplaces in *Loomis v. Amazon.com LLC*.² In *Loomis*, the plaintiff purchased a hoverboard from a third-party seller on the Amazon marketplace. Unlike the purchase in *Bolger*, however, the hoverboard in *Loomis* was not part of the FBA program, but was instead stored and shipped directly from the third-party seller to the plaintiff. Amazon's role was

limited to hosting the product on its marketplace and collecting a fee for connecting the seller and buyer. The hoverboard later caught fire, causing property damage and personal injury to the plaintiff.

Despite Amazon's exercising significantly less control over the hoverboard than the battery at issue in *Bolger*, the appellate court overturned a summary judgment ruling in favor of Amazon. The fact that Amazon "did not hold title to the product and did not have physical possession of the hoverboard does not automatically render it solely a service provider and remove it from strict liability." Amazon's marketplace remained a "direct link" in the vertical chain of distribution and had placed itself squarely between the seller and buyer. In this "gatekeeper" role, Amazon was ideally situated in the stream of commerce to exert pressure on third-party sellers to enhance safety while also allocating the costs of consumer protection through its fees, indemnity requirements and insurance.

By classifying Amazon as a seller of the defective hoverboard even when it did not exert physical control over the product, *Loomis* significantly expanded the scope of conduct through which a digital marketplace could be liable in the same way as a traditional retailer. In June 2022, a New Jersey federal



district court reached the same conclusion in *New Jersey Mfg. Ins. Grp. a/s/o Sigismondi v. Amazon.com, Inc (Sigismondi)*.³

In *Sigismondi*, a hoverboard sold by a third party on Amazon's marketplace caught fire, damaging the plaintiff's home. As in *Loomis*, the hoverboard was not part of Amazon's FBA program, but was instead shipped directly from the third-party seller to the buyer. The court analyzed whether Amazon could be considered the hoverboard's seller under New Jersey products liability law, which allows for strict liability actions against any entity in a product's

chain of distribution. As the Amazon marketplace served as the "only conduit" between the third-party seller and the buyer, the court concluded that Amazon was directly involved in placing the defective hoverboard into the stream of commerce and could be held liable as a product seller.

Implications and Considerations for Digital Marketplaces

Few digital marketplaces have the scope and breadth of the Amazon marketplace, or the logistical depth and capacity of the FBA program. In that sense, the practical implications of the *Bolger* decision were arguably limited to the unique circumstances of the Amazon marketplace. But by finding Amazon could be liable as a seller even when it did not "control" the product, the decisions in *Loomis* and *Sigismondi* significantly expand the type and scope of transactions through which a digital marketplace can be liable to the same extent as a traditional online retailer. This dramatically effects the risk and liability calculus for any digital marketplace operating in California or New Jersey. Even retailers who follow a dropship model—advertising and selling third-party products while leaving the design, manufacture, storage and shipping of those products to those third parties—could be held strictly liable for defective products.

Whether *Loomis* and *Sigismondi* represent a sea change in products liability law remains to be seen. Other jurisdictions do continue to hold that digital marketplaces cannot be held liable as sellers of third-party defective products.⁴ But as the law on digital marketplaces continues to evolve, the standard of liability expressed in *Loomis* and *Sigismondi* is likely to become increasingly attractive for both courts and legislatures, especially in jurisdictions with a history of aggressive consumer protection.

As digital commerce's share of the retail economy continues to grow and supply chains become increasingly globalized, every online retailer, big and small, needs to be aware of the risks posed by a patchwork regime of digital marketplace liability. Retailers should also be cognizant of the product safety policies and insurance requirements of suppliers and third-party sellers and should carefully review the indemnity and risk-shifting provisions of all supply contracts.



Alexandra Cunningham and Grant Cokeley

Ali is a partner and co-head of the product liability and mass tort litigation practice, and Grant is an associate in the product liability and mass tort litigation practice in the firm's Richmond office.

¹ 53 Cal.App.5th 431 (Cal Ct. App 2020). One year before *Bolger* was decided a panel of the Third Circuit found that Amazon could be held strictly liable for injuries caused by a third party's defective dog leash. *Oberdorf v. Amazon*, 930 F.3d 136 (3rd Cir. 2019). The decision attracted enough criticism that the Third Circuit *en banc* vacated the ruling and certified the question to the Pennsylvania Supreme Court. The case settled before that court could make a ruling.

² 63 Cal.App.5th 466 (Cal. Ct. App. 2021).

³ 2022 WL 2357430 (D. N.J. June 29, 2022).

⁴ See, e.g., *Amazon.com, Inc. v. McMillan*, 625 S.W.3d 101 (Tx. 2021).



Following on the FTC's Heels, Plaintiffs' Firms File Dozens of Class Actions Against Retailers and Manufacturers Alleging Technical Violations of the Magnuson-Moss Warranty Act

Plaintiffs' firms filed a spate of consumer class actions in 2022 against retailers alleging violations of the Magnuson-Moss Warranty Act's (MMWA) Pre-Sale Availability Rule and against warrantors for allegedly violating the MMWA's Anti-Tying Rule. Retailers and warrantors are currently fighting those actions in state and federal courts across the country, including an appeal to the Eighth Circuit.



The MMWA's Pre-Sale Availability Rule requires: "the seller of a consumer product with a written warranty shall make a text of the warranty readily available for examination by the prospective buyer by: (1) Displaying it in close proximity to the warranted product ... or (2) Furnishing it upon request prior to sale ... and placing signs reasonably calculated to elicit the prospective buyer's attention in prominent locations in the store or department advising such prospective buyers of the availability of warranties upon request." 16 C.F.R. § 702.3. Plaintiffs in these suits allege that retailers are failing to make product warranties available to consumers prior to purchase, thereby violating the MMWA.

The MMWA's Anti-Tying Rule, on the other hand, limits a warrantor's ability to steer consumers to manufacturer-affiliated repair shops. Specifically, it prohibits warrantors from "condition[ing]" the product warranty on the consumer's use of a name-brand "article or service" in connection with the product, unless that article or service is provided for free under the warranty. 15 U.S.C. § 2302(c). The FTC has promulgated a regulation implementing this rule that specifically prohibits product warranties that become void if the consumer seeks a repair from a nonauthorized servicer, or uses parts not manufactured by the warrantor. Several plaintiffs' firms filed putative class actions alleging violations of the MMWA's Anti-Tying Rule after the FTC published a report

on repair restrictions last year. See F.T.C., *Nixing the Fix: An FTC Report to Congress on Repair Restrictions* (2021). Plaintiffs in these suits allege that warrantors improperly condition the validity of their product warranties on the use of only authorized repair products and services. Plaintiffs claim that warrantors indicate, explicitly or implicitly, that a consumer's use of third-party repair products or services will void the product warranty, in violation of the MMWA's Anti-Tying Rule. As a result, plaintiffs allege that consumers are less likely to seek repairs from independent repair providers, which drives up repair costs by allowing warrantors to establish a monopoly over the aftermarket for product repairs.

Cases involving the MMWA's Pre-Sale Availability Rule and Anti-Tying Rule are currently pending in state and federal courts across the country, including several in the Eastern District of Arkansas. In *Leflar v. HP, Inc.*, No. 4:22-CV-00690-BRW (E.D. Ark. Oct. 4, 2022), plaintiff lodged a class action against HP in Arkansas state court, alleging that HP's product warranties violate the Anti-Tying Rule of the MMWA. In *Leflar v. Target Corp.*, No. 4:22-CV-00727-BRW (E.D. Ark. Oct. 15, 2022), plaintiff filed a putative class action against Target, also in Arkansas state court, alleging that Target failed to provide consumers with pre-sale access to warranties for its retail products, in violation of the MMWA's Pre-Sale Availability

Rule. After HP and Target removed to federal court, plaintiffs moved to remand the cases back to state court. The district court determined that CAFA could support federal jurisdiction over an MMWA action but nevertheless remanded the cases after finding that HP and Target had not met their burden of showing the amount in controversy exceeded \$5 million. Target filed a petition for permission to appeal the remand order, and the Eighth Circuit granted the petition. A decision on the appeal is expected soon, and several other MMWA actions in the Eastern District of Arkansas have been stayed pending the Eighth Circuit's ruling.



Michael Mueller, Ryan Phair, Thomas Waskom and Nicholas Drews
Mike is a partner in the commercial litigation practice in the firm's Washington, DC office. Ryan is a partner and co-chair of the antitrust and consumer protection practice and the retail and consumer products industry group in the Washington, DC office. Tom is a partner in the product liability and mass tort litigation practice in the firm's Richmond office. Nick is an associate in the antitrust and consumer protection practice in the firm's Washington, DC office.

Significant client relationships with half of the **20** largest retailers on the National Retail Federation's Top **100** Retailers List, representing retailers responsible for more than **\$1 trillion** in US sales during 2021, including the two largest retailers in the country

2022 Litigation Trends for PFAS-Containing Consumer Products and 2023 Preview

As already detailed in this Year in Review, the frenzy of regulatory activity involving per- and polyfluoroalkyl substances (PFAS) continued in earnest in 2022. The same is true for PFAS-related litigation. The focus of the litigation to date has been primarily environmental, arising from alleged contamination of drinking water sources. Lawsuits have been filed by individuals, water authorities, and states and municipalities against PFAS and PFAS-containing product manufacturers, site owners and others to recover for property damage and environmental cleanup—and in some instances, for medical monitoring.

In 2019, we also began to see filings related to PFAS in consumer products. This trend has since continued, with claim filings—primarily putative class actions—increasing in 2022. To be clear, these lawsuits do not allege personal injury or even any actual exposure to PFAS. Instead, they allege

that manufacturers and/or retailers failed to inform consumers that their products contained PFAS—or that the presence of PFAS rendered certain marketing claims (e.g., “all natural”) untrue—and thus violated state consumer protection statutes and amounted to false advertising, fraud, breach of warranty and the like. To date, an array of consumer products have been targeted, including dental floss, disposables plates and bowls and other food contact products, clothing, cosmetics and car seats. Likewise, various categories of defendants have been named, including product manufacturers and retailers.

These claims are just the latest example of a growing trend by opportunistic plaintiffs’ firms to attempt to cash in on findings of trace amounts of chemicals in consumer products, despite the absence of any actual or potential harm. A series of similar lawsuits were



recently brought following reports of trace amounts of benzene in aerosolized personal care products, including dry shampoo, hair spray, deodorant and sunscreen. The cases often follow plaintiff-funded or consumer advocacy group product testing that is then widely circulated for national media attention. The available damages generally amount to very little on an individual claimant basis, but because they can be brought as class actions (unlike personal injury claims) and carry the potential for substantial attorneys' fees and statutory treble damages, a cottage industry of plaintiffs' firms has emerged to pursue them when traditional tort claims cannot be made.

Despite the increase in claims, PFAS-related consumer product litigation is still in its infancy, and as such, its future trajectory is unclear. For example, to date, these claims have been filed by only a handful of plaintiffs' firms and in only a few jurisdictions, including primarily federal courts in California, New York and Illinois. We have not yet seen large numbers of plaintiffs' firms jump on the filing bandwagon or a proliferation of claims nationally.

Additionally, it remains to be seen whether the claims will progress substantively. The earliest claims filed in 2019 and 2020 either resolved or were otherwise voluntarily dismissed at the

pleading stage. Likewise, currently pending claims are still largely in the motion to dismiss stage, and courts have not yet decided whether claims will proceed to discovery.

That said, the first opinion we have seen in these cases was recently issued by the U.S.D.C. for the Eastern District of Pennsylvania in *Seidl v. Artsana USA, Inc.*, No. 5:22-cv-2586 (Nov. 30, 2022), which dismissed the claims at issue in their entirety. The plaintiff alleged that PFAS were present in a Chicco car seat that she purchased. Because plaintiff believed she had paid a premium for a car seat that was "chemical free," she brought claims for violation of

state consumer protection statutes, fraud, misrepresentation, breach of express and implied warranty, and unjust enrichment. Defendant moved to dismiss on the grounds that plaintiff (1) had not suffered an injury and thus did not have standing and (2) failed to state a claim on any of the legal theories asserted.

The court disagreed on the first point, finding that plaintiff had sufficiently alleged economic harm, but agreed on the second. Initially, the court found that defendant was not under any legal obligation to disclose the presence of PFAS in its car seats, and as a result, its alleged failure to do so was not sufficient to support plaintiff's claims. The court then assessed the defendant's alleged misrepresentation that the car seat did not contain PFAS. The court found that plaintiff failed to allege that she relied on any of defendant's purportedly defective statements in advance of purchasing the car seat, and thus, dismissed her statutory, fraud and misrepresentation claims. The court also dismissed the warranty claims after finding that plaintiff

failed to provide the requisite pre-suit notice of breach. Finally, the court dismissed plaintiff's unjust enrichment claim as derivative of her other claims, and thus failing for the same reasons. Although *Seidl* is a positive win for defendants, it is possible that other plaintiffs will be able to more effectively plead their claims and that nuances of state law in other jurisdictions could impact outcomes.

Another important trend to watch in 2023 is the viability of claims for medical monitoring in this context. Although plaintiffs do not allege that they have suffered health effects from exposure to PFAS, they nonetheless seek damages for ongoing monitoring for personal injuries. If allowed to proceed, these claims have the potential to drive up consumer product case values beyond those asserting mere economic harm.

To minimize litigation risk in this area, retailers should obtain assurances from their suppliers that products comply with all regulations relevant to PFAS in consumer products, and further

that all marketing claims have been vetted to account for the ubiquitous presence of PFAS throughout society. Retailers should also assess supplier indemnity provisions to ensure that they extend to these product claims. Retailers might also consider opportunities for pursuing state-level reform measures that would prevent essentially no-injury class claims like these. Finally, retailers should be prepared to aggressively defend any consumer claims they face, with the goal of discouraging similar claims from escalating into the next tort litigation wave.



Alexandra Cunningham and Merideth Daly

Ali is a partner and co-head of the product liability and mass tort litigation practice, and Merideth is partner in the product liability and mass tort litigation practice in the firm's Richmond office.

300+ lawyers
across **20** practices
serving our retail
and consumer
products clients

Check Your Inventory; Do You Have Enough Cyber Insurance?

The COVID-19 pandemic transformed or outright upended almost all aspects of life, and retail was not immune to that disruption. Retailers slow to adapt to digital technologies suddenly scrambled to adopt contactless payment, curbside pickup and a myriad of other developments required by a homebound consumer base. While lockdowns are largely over, digitization and the technological progress accelerated by COVID-19 are here to stay as consumer preferences have evolved in favor of these operational advancements. Yet while digitization enabled businesses to survive—and even thrive—during the pandemic, now that the rush is over, retailers must assess the complex and significant risks these new processes pose, as well as the insurance coverages needed to address those risks, which include ransomware attacks and data breaches, spyware and malware and myriad other risks that simply did not garner the same level of attention in the pre-pandemic era.

The Retail Trend Towards Digitization

Although online shopping predated the pandemic, COVID-19 took it to new heights—in 2020, an additional \$900 billion was spent in online retail compared to 2019.¹ Mastercard estimates that roughly 20-30 percent of that shift is expected to be permanent. Yet brick-and-mortar retailers, from small businesses to global behemoths like Walmart and Target, have tapped into the online shopping boom, integrating the in-person and online experience with services such as curbside pickup and virtual “try ons.” A consumer can now order a pair of shoes on a mobile app and drive to the store and pick them up the same day. In some cases, the customer may not even need to interact with a retail employee before walking out the door with her goods.

Even the traditional in-store shopping experience has undergone a digital upgrade. Amazon/Whole Foods offers contactless checkout at select stores. Nearly all

major retailers offer either a “tap” or “scan” to pay feature that has the consumer pulling out a smartphone instead of a wallet. And in some cases, in-store shoppers will experience augmented reality (AR) or artificial intelligence. For example, a shopper can scan an image of a dress in the store and see an overlay showing that item paired with corresponding accessories. Clothing retailer Uniqlo offers customers the option to try on one item in various colors with its AR mirrors.

As a result of and in conjunction with these digitization efforts, retailers are amassing swaths of consumer data—not just names, email addresses and payment information, but personal preferences and characteristics. Retailers can mine this information to segment their customer base and offer targeted marketing campaigns, personalized social media ads and enhanced loyalty programs. Consumer data is often stored in cloud-based technology that enables the retailer to seamlessly integrate the various platforms from which customers shop for its products. While this data provides invaluable marketing opportunities, it also poses major risks that traditional insurance products may not cover.

Balancing Digitization and Cybersecurity

As the use of digital technology and the collection of consumer data increases, it becomes even more important for retailers to identify the potential risks that arise and ensure the appropriate insurance coverage is in place, namely a robust cyber insurance policy to protect against the risk of computer network interruption or a data or privacy breach.

Contactless payment systems allow for a faster checkout time, but these systems work only if a retailer’s computer network is operating. If the network servicing the retailer’s application or the network servicing the payment system goes down or is interrupted, the retailer could suffer significant loss of business and loss of profits. While a retailer will typically have “business interruption” or “loss of business” insurance for lost profits and extra expenses related to a suspension of operations, insurers will certainly argue, and some courts may agree, that traditional business interruption coverage does not cover a network outage or interruption caused by a ransomware attack or other cyber-related outage that does not result from a physical loss or damage to tangible property. See,

¹ “Mastercard Recovery Insights: E-commerce a COVID lifeline for retailers with additional \$900 billion spent online globally,” (Apr. 6, 2021), available at <https://www.mastercard.com/news/press/2021/april/mastercard-recovery-insights-e-commerce-a-covid-lifeline-for-retailers-with-additional-900-billion-spent-online-globally/>.

e.g., *EMOI Services, L.L.C. v. Owners Ins. Co.*, Slip Op. No. 2022-Ohio-4649 ¶ 16 (Dec. 27, 2022) (finding “[c]omputer software cannot experience ‘direct physical loss or physical damage’ because it does not have a physical existence.”) A retailer would need to secure specific cyber-related insurance coverage for this risk.

As another example, if a retailer relies on a third-party provider to operate its digital app or contactless payment system, it should consider securing contingent business interruption coverage, which covers a retailer’s lost profits resulting from the interruption of another business’s operations that the retailer relies on, such as a retailer’s key supplier. Contingent business interruption coverage, however, also typically requires direct physical loss to the third party, so a retailer will need to secure coverage under a cyber-specific policy to specifically cover lost profits resulting from the interruption of a third-party service provider because of a ransomware attack or other cyber-related incident.

Retailers also are at risk of liability from unauthorized disclosure of customer information. With increasing amounts of customer data being collected and utilized in electronic payment systems, a breach of those systems can have devastating and immediate consequences, both financial and reputational. A robust cyber insurance policy can also address this potential liability by providing coverage for breach notification costs, credit monitoring costs, public relations expenses and other costs resulting from a data breach.

The patchwork of state consumer and privacy laws, with varying triggers from state to state as to what constitutes personal information and requirements for notifying impacted individuals, necessitates the use of breach response counsel to thoughtfully guide a retailer through cyber incident response, including navigating the local, state and federal regulations and requirements. The legal fees for breach counsel and any third-party vendors they retain, such as a forensic investigator to determine the scope and extent of the

incident and possibly a public relations firm to mitigate the reputational harm to the retailer, can be significant, but a good cyber insurance policy provides coverage for these costs.

Even if a retailer relies on a third party to handle all aspects of the retailer’s contactless payment or other digitization system, if there is a data breach or other unauthorized disclosure, the retailer still faces a significant risk that it will be embroiled in third-party lawsuits. Thus, in addition to making sure that it has adequate insurance coverage for a cyber incident, a retailer must also ensure that any third party it relies on also has adequate insurance coverage for these losses, including liability for a privacy breach and breach notification costs.

Conclusion

While retailers continue to embrace emerging digitization to streamline and enhance the buying experience, retailers must identify all potential liability risks arising from these technologies to ensure that their insurance coverage adequately covers those risks and potential exposure to a cyber-related loss.



Michael Levine, Latosha Ellis, Janine Hanrahan
Michael is a partner and Latosha is counsel in the insurance coverage practice in the firm’s Washington, DC office. Janine is an associate in the insurance coverage practice in the firm’s Boston office.



“ They are very practical in their advice and have a good sense of what regulators and consumers really care about. ”

Chambers USA

“ The [retail] team’s strength lies in its business-friendly approach. ”

Chambers USA



Accountability in Cybersecurity and Privacy: Keeping Your Name Out of the Headlines

In the United States, recent legal actions and regulatory developments suggest a growing emphasis on accountability at the senior leadership level for companies' cybersecurity and privacy practices. In particular, the Federal Trade Commission (FTC) has more frequently found company executives individually liable for their company's alleged cybersecurity and privacy failures, including a failure to implement (or properly delegate the responsibility to implement) reasonable information security practices. Separately, certain federal and state regulators have proposed new requirements focused on increasing senior leaders' awareness, governance and oversight of cybersecurity-related issues.



FTC Holds Executives Individually Liable

Pursuant to Section 5 of the FTC Act, the FTC has the authority to prohibit "any ... unfair or deceptive act or practice in or affecting commerce." Although the FTC Act does not address cybersecurity or privacy specifically, the act provides the vehicle through which the FTC can investigate and bring enforcement actions against companies whose cybersecurity and privacy-related business practices are considered unfair or deceptive. In fashioning relief for a Section 5 violation, the FTC has broad remedial discretion and can impose continuing obligations to safeguard the security and privacy of personal information and enjoin future misconduct.

Historically, the FTC has only occasionally sought to hold executives individually liable in connection with privacy or data security enforcement actions. For example, in 2015, the FTC settled with Atlanta-based medical billing company PaymentsMD and its former CEO Michael C. Hughes for privacy-related issues, including for allegedly collecting customers' medical data without obtaining consent.¹ In contrast, the FTC's \$5 billion settlement with Facebook

¹ In the Matter of PaymentsMD, LLC, Docket No. C-4505.

in 2019 did not hold CEO Mark Zuckerberg individually liable for Facebook’s violation of a prior FTC consent order to better protect user privacy. The FTC, however, did order Mr. Zuckerberg to be relieved of his authority over Facebook’s privacy decisions and for a board of directors-level committee to be established and tasked with improving transparency and accountability with respect to the company’s privacy practices. FTC Commissioner Rohit Chopra wrote a dissent to the settlement, suggesting that executive-level accountability may have been part of the FTC’s internal deliberations.

Beginning in late 2021, however, the FTC started to more frequently use its authority to find company executives individually liable. Notably, on September 1, 2021, the FTC announced it had permanently banned Support King, LLC (d/b/a SpyFone.com) and its CEO Scott Zuckerman from the surveillance business over

allegations that (1) the company’s “stalkerware” app secretly collected and shared data on people’s physical movements, phone use and online activities through a hidden device hack and (2) the company failed to implement basic security features, which exposed device owners to hackers, identity thieves and other cyber threats. The FTC named Zuckerman as a defendant in both an individual and corporate officer capacity and, among other restrictions, permanently prohibited Zuckermann from misrepresenting “the extent to which [Zuckerman and SpyFone] maintain and protect the privacy, security, confidentiality, or integrity of [p]ersonal [i]nformation.” In addition, the FTC required “any business that [Zuckerman] controls, directly or indirectly” to (1) implement an information security program, (2) obtain initial and biennial information security assessments performed by a third party,

(3) annually certify compliance with the settlement order and (4) report data breaches to the FTC within 21 days of notifying other government entities.²

Similarly, on October 5, 2021, the FTC finalized a settlement involving the now-defunct MoviePass for allegedly deceptive practices and a failure to secure subscribers’ personal data. According to the FTC, MoviePass “left a database containing large amounts of subscribers’ personal information unencrypted and exposed, leading to unauthorized access.” The FTC named both the CEO of MoviePass, Mitchell Lowe, and the CEO of MoviePass’ parent company, Theodore Farnsworth, as defendants in both an individual and corporate officer capacity. Similar to the SpyFone enforcement action, the FTC order (1) permanently barred Lowe and Farnsworth from misrepresenting their businesses and data security practices, (2) required any

businesses controlled by Lowe or Farnsworth to implement comprehensive information security programs and obtain information security assessments performed by third parties and (3) required “any business that [Lowe or Farnsworth] controls, directly or indirectly” to notify the FTC of any future data breaches within 30 days of discovering the breach.³

More recently, on January 9, 2023, the FTC finalized an order against Drizly, an online alcohol ordering and delivery service, and its CEO James Cory Rellas for an alleged failure to maintain appropriate security safeguards that led to a data breach affecting 2.5 million consumers’ personal information. The FTC named Rellas as a defendant in both an individual and corporate officer capacity and alleged that he was personally responsible for the company’s security failures by not properly implementing (or delegating the responsibility to implement) reasonable information security practices, such as by failing to hire a senior executive responsible for the security of consumers’ personal information. The order requires Rellas to implement an information security program at any future

company (that collects personal information of more than 25,000 individuals) at which he serves as a majority owner, CEO or senior officer with information security responsibilities.⁴ Commenting on the case, FTC Chair Lina Khan stated, “I think we’ve also seen that there are certain sectors in which there’s a lot of turnover, especially in the tech sector, where executives are kind of jumping from company to company. And so, we wanted to make sure that the lessons from this were attaching, no matter where the executive went.”⁵ In its press release on the matter, the FTC admitted that the Drizly outcome is part of the FTC’s efforts to ensure that “careless CEOs learn from their data security failures.”⁶

Executive Faces Criminal Prosecution

Most regulatory enforcement and litigation related to cybersecurity and privacy issues have involved civil liability. In 2022, however, there was the first-ever criminal conviction of a company executive in connection with the handling of a data breach. On October 5, 2022, former Uber Chief Security Officer Joe Sullivan was found guilty by a jury in US federal court for his

alleged failure to disclose a 2016 breach of Uber customer and driver data to the FTC in the midst of a then-ongoing FTC investigation into the company. Sullivan was charged with one count of obstructing an FTC investigation and one count of misprision (the act of concealing a felony from authorities) and was convicted on both counts. The government alleged that, in 2016 as the FTC already was investigating Uber for a 2014 data breach, Sullivan learned of a new breach that affected the personal information of more than 57 million Uber customers and drivers. Hackers allegedly demanded a ransom of at least \$100,000 from Uber, and instead of reporting the new breach to the FTC, Sullivan and his team allegedly paid the ransom and had the hackers sign a nondisclosure agreement. Sullivan also allegedly did not report the breach to Uber’s general counsel. Uber did not publicly disclose the incident or inform the FTC of the incident until 2017, when a new chief executive officer joined the company.⁷ At the time of this publication, a sentencing date for Sullivan had not yet been set.⁸

2 In the Matter of Support King, LLC d/b/a SpyFone.com and Scott Zuckerman, Docket No. C-4756.

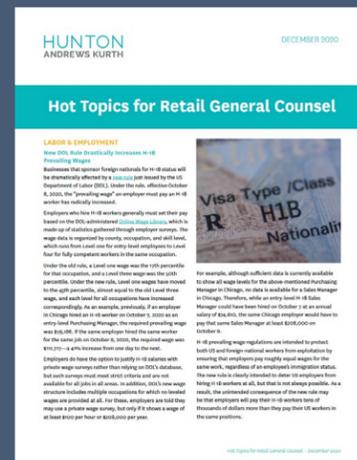
3 In the Matter of MoviePass, Inc., Helios and Matheson Analytics, Inc., Mitchell Lowe, and Theodore Farnsworth, Docket No. C-4751.
 4 In the Matter of Drizly, LLC and James Cory Rellas, Docket No. C-4780.
 5 “FTC Chair Lina Khan Discusses Accountability for Violations of Agency Rule,” Wall Street Journal, <https://www.wsj.com/livecoverage/wsj-ceo-council-2022/card/ftc-chair-lina-khan-discusses-accountability-for-agency-s-rule-violations-V9uMEyp0lemdmkPCvCIW>.
 6 “FTC Takes Action Against Drizly and its CEO James Cory Rellas for Security Failures that Exposed Data of 2.5 Million Consumers,” FTC press release, <https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-takes-action-against-drizly-its-ceo-james-cory-rellas-security-failures-exposed-data-25-million>.
 7 In the Matter of Uber Technologies, Inc., Docket No. C-4662.
 8 “Former Chief Security Officer Of Uber Convicted Of Federal Charges For Covering Up Data Breach Involving Millions Of Uber User Records,” US Department of Justice press release, <https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-convicted-federal-charges-covering-data-breach>.

Client Resource

GC Hot Topics Memo

Hunton Andrews Kurth is pleased to provide an informative communication focused on the issues facing retail General Counsel. This quarterly publication features items on advertising, antitrust, consumer health and safety, corporate governance and securities disclosure, immigration, insurance, intellectual property, labor and employment, privacy and cybersecurity, and retail finance.

Easy-to-read and focused on the latest hot topics, if you are interested, please email our editor Phyllis Marcus at pmarcus@HuntonAK.com to receive the next publication.



Partner Phyllis Marcus named to the National Law Journal's 2023 list of Media and Advertisement Law Trailblazers

New Regulatory Requirements

Several regulatory bodies at both the federal and state levels have taken up rulemakings aimed specifically at strengthening cybersecurity governance and oversight mechanisms and ensuring that senior leadership and boards of directors possess the requisite expertise to carry out such responsibilities. For example, the FTC's Gramm-Leach-Bliley Act (GLB) Safeguards Rule, the Securities and Exchange Commission's (SEC) Cybersecurity Rules and the New York Department of Financial Services (NYDFS) Part 500 Cybersecurity Rules all similarly impose requirements on senior leadership to ensure they play an active role in reviewing and implementing a company's cybersecurity program.

FTC: In 2021, the FTC announced amendments to its GLB Safeguards Rule, which already obligates covered financial institutions to develop, implement and maintain a comprehensive information security program. The amendments to the Safeguard Rules would require a financial institution to, among other requirements, (1) designate a "qualified individual" to oversee, implement and enforce the institution's information security program and (2) submit periodic reports to the institution's board of directors or an equivalent governing body addressing, among other subjects, the status of the institution's information security program, recommended changes to the program and the institution's compliance with the Safeguards Rule. The effective date of these new requirements is June 9, 2023.

SEC: A new set of rules proposed by the SEC in March 2022 would amend Form 8-K to impose new reporting obligations with respect to material cybersecurity incidents and cybersecurity risk management, strategy and governance, each as specified in Items 106(b), 106(c) and 407 of Regulation S-K. Specifically, Proposed Item 106(b) would require a public company to disclose its policies and procedures, if any, to identify and manage cybersecurity risks and threats. Proposed Item 106(c) would require disclosure of a public company's cybersecurity governance practices, including a description of the board

of directors' oversight of cybersecurity risks management's role in assessing and managing cybersecurity risks, the relevant expertise of such management and its role in implementing the company's cybersecurity policies, procedures and strategies. In addition, amendments to existing Item 407 would require a public company to disclose the name of any member of the board of directors who has cybersecurity experience and provide details as necessary to fully describe the nature of such expertise.

NYDFS: NYDFS's proposed amendments to NYDFS Part 500 Cybersecurity Regulations would require that a "qualified individual," responsible for overseeing, implementing and enforcing a covered entity's cybersecurity program, have adequate independence and authority to ensure cybersecurity risks are appropriately managed. In addition, the qualified individual would be required to timely report material cybersecurity issues to a "senior governing body" that, in turn, would be responsible for reviewing and approving the covered entity's cybersecurity policies at least annually. Further, if the covered entity has a board of directors or an equivalent governing body, the board or an appropriate committee thereof must (1) exercise oversight of, and provide direction to management on, cybersecurity risk management, (2) require executive management or its delegates to develop, implement and maintain the covered entity's cybersecurity program and (3) possess sufficient expertise and knowledge (or be advised by someone with such expertise and knowledge) to provide effective oversight of cybersecurity risk management.

Looking Ahead to 2023

Heading into 2023, we expect both the FTC's focus on holding executives individually liable for companies' cybersecurity and privacy shortcomings, and regulators interest in setting forth requirements regarding cybersecurity governance and oversight, to continue. Retailers therefore should be prepared to focus effort in this space, ensuring that those in leadership have the expertise necessary to maintain reasonable cybersecurity and privacy programs and that governance mechanisms are in place, and periodically reviewed and tested, to ensure cybersecurity and privacy issues are adequately addressed when they arise.



**Aaron Simpson, Michael La Marca and
Lauren Berkebile**

Aaron is a partner, Mike is counsel and Lauren is an associate in the global privacy and cybersecurity practice in the firm's New York office.

2022 Retail M&A Year in Review

Overview of 2022

Global dealmaking suffered a record fall during the second half of 2022, as rising interest rates, surging inflation and the war in Ukraine brought a period of frenetic activity to an abrupt, if not surprising, close.

According to data provider Refinitiv¹, mergers and acquisitions totaled \$3.6 trillion worldwide in 2022, down 37 percent from 2021's record-breaking level, which is the largest year-over-year percentage decline since 2001. By number of worldwide deals, nearly 55,000 deals were announced in 2022, a decrease of 17 percent from 2021 and a two-year low.

M&A activity began its plunge in May, as recessionary headwinds gathered strength. Between the first and second halves of 2022, total worldwide M&A activity totaled \$1.4 trillion, a 33 percent decline compared to the first half of 2022. This drop-off was the largest second-half percentage drop since records began in 1980, partly caused by a 57 percent drop in private equity activity.

The market for consumer and retail M&A was no different. Ongoing supply chain challenges, tighter financing, rising interest rates, inflation and changing consumer behaviors made companies in this sector less desirable targets. Retail deal values fell to \$121.6 billion, a decrease of 48 percent compared to 2021. Deal value in the consumer products and services dropped 44 percent compared to 2021 and deal value in consumer staples fell 37 percent.

Retail deal value would have been down even further but for the planned \$24.6 billion acquisition of Albertsons by Kroger announced in October 2022—the first, and only, retail megadeal of 2022. This would be the biggest supermarket transaction ever, besting Albertsons' buyout by a Cerberus-led consortium for \$17.4 billion in 2006, Amazon's \$13.7 billion deal for Whole Foods Market in 2017 and Kroger's \$13.5 billion acquisition of Fred Meyer in 1998.²

Like the broader M&A market, the number of consumer and retail deals

¹ <https://thesource.lseg.com/thesource/getfile/index/78b4d1a3-f045-46ec-8fc6-e1f685505a9c>

² <https://community.ionanalytics.com/retail-therapy>

was down significantly from 2021, with a 24 percent decrease in the retail market, a 14 percent decrease in the consumer products and services market and a 19 percent decrease in the consumer staples market.

Conversely, the discount and department store retailing sector and the household and personal products sector rallied, with deal values over 2021 increasing 158 percent in the discount and department store sector and 55 percent in the household and personal products sector.

One manifestation of these challenging deal conditions was the abandoned M&A process for department store chain Kohl's. Kohl's was in sale talks with Franchise Group, but terminated

the deal in late June, after cutting its outlook for the second quarter, citing softer consumer spending amid decades-high inflation.³

At first blush, it may look like the sky fell on the M&A market in 2022. It is a compelling headline, but the bigger picture shows an active M&A market that is in line with healthy, pre-COVID levels. The activity levels of 2021 were unsustainable and a correction was inevitable. The question is now to what degree this new business climate—one where short-term volatility in financial markets, inflationary pressures, soaring borrowing costs, supply chain disruptions and geopolitical tensions all appear to be developing into longer-term trends—will continue to slow M&A deal activity.

Looking Forward to 2023

Though consumer and retail, particularly brick-and-mortar, continue to face headwinds in consumer confidence, inflationary pressures, excess inventories and continued labor shortages in 2023, we nonetheless expect that consumer and retail M&A will continue at “normal” (i.e., pre-COVID) levels in 2023. M&A will continue to be an indispensable tool for companies seeking to transform business models and reposition themselves for future growth as consumer behavior rapidly evolves in a post-pandemic world. However, we anticipate that the sluggishness of the second half of 2022 will continue into the first half of 2023 until economic uncertainty dissipates.

Smaller Deals: We expect small and midsize deal activity to continue to be strong in 2023, while major retail acquisitions, particularly those involving publicly traded companies exposed to recent market volatility, may lag behind in light of recent unsuccessful sale processes, antitrust concerns and high financing costs. In lieu of major acquisitions, smaller bolt-on acquisitions, joint ventures or minority interests may be an effective way to acquire on-strategy capabilities or an expansion outside of core competencies. On the sell-side, we think companies will continue divesting underperforming or noncore assets.

Distressed Assets: In the United States, distressed retail M&A activity was very slow in 2022, with retail bankruptcies at a decade-low level. However, we expect that distressed M&A activity will increase in 2023, as difficult market conditions continue to affect liquidity and companies' ability to refinance upcoming debt maturities. As distressed retailers struggle to maintain their current financial structures, retailers with strong balance sheets will have the opportunity to purchase distressed

assets at discounted prices. An increase in distressed sellers should also create more opportunities for private equity buyers, which remain well-capitalized with ample dry power. Globally, these funds are estimated to have \$1.68 trillion at their disposal across strategies and approximately half of that is sitting in North American funds.⁴

E-commerce: Even though e-commerce growth has slowed since the height of the pandemic,⁵ the future of retail will continue to be a blended experience of online and in-person. For brick-and-mortar retailers falling behind, acquisition may represent an efficient way to rapidly build digital capabilities, rather than attempting to build those capabilities in-house on an accelerated time frame, particularly at a time when valuations may be more palatable.

ESG: Increasing consumer commitment to social responsibilities, including environmental, social and governance (ESG) and diversity, equity and inclusion (DE&I), presents an opportunity for investment and acquisitions into sustainable business models and

brands. For example, some grocery retailers have acquired waste management companies to reduce, reuse and recycle waste.

Antitrust Scrutiny: Retail M&A will continue to face antitrust scrutiny as a result of high inflation and vocal consumer unrest about rising prices across the board. For example, Albertsons' proposed merger with Kroger has garnered intense scrutiny from regulators and state attorneys general.



James Kennedy

Jim is a partner in the mergers and acquisitions practice in the firm's Richmond office.

³ <https://www.cnbc.com/2022/06/30/kohls-terminates-sale-talks-with-franchise-group.html>

⁴ <https://www.datasite.com/us/en/resources/insights/reports/deal-drivers-americas-2023-outlook.html>

⁵ <https://www.adweek.com/commerce/pandemic-e-commerce-americans-bought-so-much-stuff-online-it-was-basically-another-holiday-season/>

Represent more than
500 retail and consumer
products clients



Getting Hot in Here: Workplace Safety Regulators Address Employee Heat Illnesses

Federal and state safety regulators are turning up the heat to make sure employees can keep cool.

The Occupational Safety and Health Administration (OSHA) is developing a new standard to regulate heat illnesses at work. OSHA published an Advance Notice of Proposed Rulemaking in late 2021 notifying stakeholders of its intent to regulate heat exposure in both indoor and outdoor work environments. See 86 Fed. Reg. 59309 (Oct. 27, 2021). The comment period closed on January 26, 2022. The agency appears poised to release a draft rule at some point during 2023. If a final rule is promulgated, it will represent the first time that federal OSHA imposed specific standards related to workplace exposure to heat hazards.



Currently, California, Washington, Oregon and Minnesota have their own state-plan regulations for heat safety. Other state plans and federal OSHA use the General Duty Clause (or state equivalent) to cite employers for exposing employees to heat-related hazards. The General Duty Clause is found in Section 5(a)(1) of the OSH Act and requires employers to provide employment and a place of employment “free from recognized hazards that are causing or are likely to cause death or serious physical harm.”

For retailers, the federal heat standard has potentially wide-reaching application. Work that is exclusively outdoors obviously will be covered. The rule also is likely to impact loading docks, warehouses or other workspaces that provide at least some exposure to outdoor working conditions. Specialty retailers and big-box retailers with landscaping and gardening sections that require employees to work outside will be covered, and likely even restaurants that offer outdoor dining or parking lot delivery. The standard also may cover retailers with exclusively indoor working environments if those areas are not climate controlled. We do not know whether OSHA also will include indoor areas that are climate controlled but still can become very hot, such as restaurant kitchens. Retailers with any work areas that can become extremely hot should make heat hazard mitigation a focus in 2023.



Hunton Andrews Kurth
named to *Global
Competition Review's*
2023 edition of its
GCR 100

Proposed Federal Heat Standard—What to Expect and When to Expect It

NIOSH updated its recommended criteria for a standard addressing occupational exposure to heat and hot environments in 2016. See <https://www.cdc.gov/niosh/docs/2016-106/>. OSHA has signaled what employers can expect in its proposed standard through its own publications and guidance, which draws on NIOSH's work. See, e.g., <https://www.osha.gov/heat-exposure>, <https://www.osha.gov/heat-exposure/rulemaking>. As such, we reasonably anticipate that the standard will include the following:

- Written heat illness prevention plan
- Engineering, administrative and personal protective equipment controls to reduce risk of heat illness among employees
- Acclimatization—or the process of allowing employees to gradually adjust to working in hot environments
- Physiologic and exposure monitoring for employees working in hot environments
- Planning and responding to heat illness emergencies, including contacting emergency response agencies and providing on-site assistance to employees before emergency services arrive
- Worker education, training and engagement on heat-related workplace risks

Representatives from OSHA have commented publicly on the difficulty of establishing specific criteria like temperature thresholds for standards to kick in because of other variables, like humidity and exposure to sunlight, that can significantly change risk of heat illness, and the agency has suffered some litigation losses due to the lack of reliable scientific measurements of risk. See, e.g., *A.H. Sturgill Roofing Co. v. Secretary of Labor*, 2019 WL 1099857 (No. 13-0224, 2019). To avoid these issues, OSHA may center the standard around general requirements, like mandatory acclimatization and access to shade and water, that can apply to all outdoor workplace settings even in moderately warm conditions and avoid a particular temperature that it asserts will establish a hazard. This approach likely would make a rule

less vulnerable to legal challenge. However, OSHA currently has a National Emphasis Program (NEP) related to heat illness, which does contain specific metrics.

The NEP was issued in 2022 and focuses on working environments that expose workers to temperatures above 80 degrees and humidity above 40 percent. The NEP instructs compliance officers conducting nonheat-related investigations to inquire about heat illness prevention plans and, if the employer has any heat-related incidents on their logs, the CSHO must open a separate heat-related inspection. The NEP also calls for programmed inspections of certain employers when the National Weather Service has announced a heat advisory or heat warning for the local area.

Existing State Heat Regulations

Some states have enacted their own standards to address heat-related hazards.

For example, California's heat illness standard applies to all outdoor work environments. It requires employers to develop heat illness prevention plans and provide all outdoor workers with potable drinking water, access to shade and cool-down breaks. The standard contains a specific acclimatization requirement that mandates supervisors to closely observe employees who are new to hot working environments for at least the first 14 days. It also requires both employee and supervisor training, and specific emergency response procedures, including mandatory reporting of heat illness symptoms to supervisors and a requirement that no employees suffering from heat illness symptoms are left alone.

Washington state maintains a similar outdoor heat standard that applies from May 1 to the end of September each year. Like California, the standard requires access to water, shade

and paid, preventative cool-down breaks in high temperatures. It also requires employee and supervisor training and for employers to develop a method for supervisors and employees to communicate about signs and symptoms of heat illness. In 2021, Washington supplemented its existing heat standard with emergency rules specifically applicable for temperatures above 89 degrees and extreme heat above 100 degrees.

Minnesota's heat standard is unique in addressing indoor work environments. The standard kicks in based on different types of work and temperature measurements. It requires employers to regulate "wet bulb globe temperatures," which measure a combination of air temperature, air speed, humidity and radiation, based on the intensity of the work at issue. For example, when employees perform "heavy work," including heavy lifting, pushing and shoveling, indoor wet bulb globe temperatures cannot exceed 77 degrees. For moderate work, the threshold rises to 80 degrees, and for light work, the highest permissible wet bulb temperature is 86 degrees. The standard most readily applies in warehouse settings without climate control, but could also apply in locations like kitchens that expose workers to hot, potentially muggy conditions.

Oregon enacted a permanent heat illness rule in May 2022. The rule applies to any workplaces where extreme heat caused by weather can expose workers to heat-related illness, but does not apply to buildings that have mechanical ventilation that keeps the indoor heat index below 80 degrees Fahrenheit. The Oregon standard requires access to shade and drinking water, supervisor and employee training, special procedures for high heat about 90 degrees, acclimatization requirements and plans for emergency medical management.



A few additional states have proposed their own heat-related regulations recently. Nevada released a draft standard in February 2022 that would require employers who have employees working in dry bulb temperatures above 90 degrees Fahrenheit to develop heat illness management programs that cover issues like access to water, rest breaks, shade and employee monitoring. It would also require training for employees and additional, more detailed training for supervisors, and mandates taking employees out of work if they showed signs of heat illness. Maryland OSHA proposed a similar standard in October 2022 that would apply to workers exposed to heat indexes greater than 88 degrees Fahrenheit for more than 15 minutes per hour. The proposed Maryland standard would also require employers to develop a heat illness management program, providing training and developing protocols for emergency response. Notably, the Maryland standard received opposition from employee groups claiming the 88 degree heat index threshold was not low enough to protect many workers.

Advice for Retailers—How to Deal with Heat

As retailers prepare for a new wave of heat safety regulations, retailers that do not yet have heat hazard mitigation programs in place should take some steps to prevent heat illness among employees. Retailers should focus on giving employees the necessary time to adapt to working in warm conditions. Most heat illnesses

and injuries, including fatalities, occur within the first 14 days after an employee transitions to hot working conditions. For this reason, acclimatization is a focus of heat illness regulation and a key part of any effective heat illness prevention program. Allowing employees to ease into hot working conditions so they can adjust slowly over time can significantly reduce the risk of heat stroke or death. Employers also should provide employees with access to drinking water and shade and encourage employees to inform their supervisors if they feel signs of heat illness like dizziness, confusion, lightheadedness, extreme sweating or cramping. Employees, particularly new employees, should know that they can report these symptoms to management without fear of retaliation or other negative workplace consequences. Educating employees about signs and symptoms of heat stroke or other heat illness can give employees the tools they need to help protect themselves when temperatures rise.



Susan Wiltsie and Reilly Moore
Susan is a partner and Reilly is an associate on the labor and employment team in the firm's Washington, DC and Richmond offices, respectively.



Labor Organizing in Retail: 2022 Review

2022 Overview of Retail Organizing

In 2022, labor organizing was in the spotlight with workers organizing at a rate not seen in years. Between October 1, 2021, and September 30, 2022—the National Labor Relations Board's (NLRB or Board) fiscal year—2,510 union representation petitions were filed.¹ This is a 53 percent increase from 2021 and is the highest number of union representation petitions filed since 2016.² Further, unions in 2022 have won the most elections since 2005.³ Among the American public, union approval is hovering around 70 percent, its highest level since 1965.⁴

The political and social issues of the last few years, inflation, the looming recession, job insecurity, wages and pandemic-related frustration/unhappiness are just a few of the countless reasons cited for the boom

in union support/approval. In addition to an increase in unionization as a whole, 2022 also produced a rise in “homegrown” unions rivaling the established bluebloods. For instance, in mid-November, more than 100 service industry workers gathered in South Carolina (the state with the country's lowest unionization rate) to formally announce the launch of a new union—the Union of Southern Service Workers (USSW). The USSW was created in an effort to increase unionization throughout the South.⁵ The USSW will prioritize the service industry as a whole, including retail.⁶ The USSW is just one of many homegrown/upstart labor unions making waves in 2022, with others including Starbucks Workers United, Trader Joe's United and New Seasons Labor Union.

¹ Of these 2,510 representation petitions, 2,072 were filed in calendar year 2022. See NLRB, *Representation Petitions – RC*, nlr.gov (last visited Dec. 23, 2022), <https://www.nlr.gov/reports/nlr-case-activity-reports/representation-cases/intake/representation-petitions-rc>.
² See NLRB, *Election Petitions Up 53%, Board Continues to Reduce Case Processing Time in FY22*, nlr.gov (Oct. 6, 2022), <https://www.nlr.gov/news-outreach/news-story/election-petitions-up-53-board-continues-to-reduce-case-processing-time-in>.
³ See Rani Molla, *How Unions Are Winning Again, In 4 Charts*, vox.com (Aug. 30, 2022), <https://www.vox.com/recode/2022/8/30/23326654/2022-union-charts-elections-wins-strikes>.
⁴ *Id.*
⁵ See James Pollard, *New Service Union Seeks to Inspire Labor Movement in South*, U.S. News (Nov. 18, 2022), <https://www.usnews.com/news/us/articles/2022-11-18/new-service-union-seeks-to-inspire-labor-movement-in-south>.
⁶ *Id.*

One lesson from 2022 is that organizing can spread like wildfire, as several industries and companies have faced or are currently facing unionization threats for the first time. This includes the retail industry, which did not escape 2022 unscathed, with several major retailers facing unionization threats despite little or no prior union history. Starbucks, REI, Target, Trader Joe's and Apple are just a few examples of retailers that faced organization efforts over the course of 2022. Notably, many of these retailers enjoy generally positive reputations and did nothing significantly "wrong" to attract unionization efforts. Additionally, with the Biden administration taking full control over the NLRB, the law has vastly evolved over the past year.

General Counsel Abruzzo's Agenda

In addition to an increase in union representation elections, 2022 also saw a policy shift favoring unions over employers. Throughout the course of his presidency, President Biden has stated on a litany of

occasions that he intends to be the "most pro-union president" in American history.⁷ Indeed, one of his first official acts as president was terminating Peter Robb, the Trump-appointed NLRB general counsel (GC), just minutes after taking the oath of office.⁸ President Biden shortly thereafter nominated Jennifer Abruzzo as Robb's successor,⁹ who was later confirmed by the Senate. While the GC does not have the power to change or make law, it does set the Board's litigation and enforcement agenda and priorities, thereby having a significant hand in shaping the nation's labor policies.

GC Abruzzo hit the ground running, quickly issuing several interpretive memoranda and otherwise signaling her intent to ask the Board to substantially overhaul well-established NLRB precedent in an effort to diminish employer rights. One of the most significant, and illustrative, memoranda GC Abruzzo has issued is Memorandum GC 22-04. GC 22-04 states that Abruzzo, as GC, would request the Board overrule long-standing precedent and hold



that employer-mandated meetings in which employers utilize their right to free speech by communicating their views and stance on unionization violates the National Labor Relations Act (NLRA). GC 22-04 asserts that, since 1948, the Board has incorrectly concluded that an employer does not violate the NLRA by requiring employees to attend these so-called "captive audience" meetings, which Abruzzo claims infringe on employees' Section 7 rights to refrain from listening to employer speech.¹⁰

This is significant because, for the past 75 years, employers have utilized these meetings to, among other things, (1) lawfully inform employees of their stance on unions; (2) address head-on any misrepresentations, rumors or other false statements being made by the union; and (3) provide employees with information about unions and the potentially negative consequences of joining a union. Because many of these negative consequences are most commonly **not** disclosed by the union, these meetings equip employees with a full understanding of what it means to unionize, thereby allowing employees to make a fully informed choice.

While GC 22-04 has yet to be tested in court, seeking to overturn 75+ years of precedent as one of her first acts as GC signifies Abruzzo's intent to rewrite federal labor law so it protects and favors unions over employers.

Changes in Law Via Board Decisions

In addition to GC Abruzzo, the Board is and will likely continue reducing employer rights through its decision making in various cases. One example of note for retailers is *Tesla*,¹¹ wherein the Board ruled that workplace dress codes and uniform policies that prevent employees from wearing pro-union apparel of any type, even if facially neutral, are presumptively unlawful unless such policies are justified by "special circumstances."¹² This is significant because the previous standard drew a distinction between an employer's complete ban on union insignia and an employer's regulation of the type and/or manner in which employees wore union insignia. But now, under *Tesla*, any union insignia donned by an employee is protected unless the employer can demonstrate that there are "special circumstances" that justify the employer's regulation of such.

Notably, this "special circumstances" exception is much harder to meet than may be facially apparent. Despite the *Tesla* Board's citing *Komatsu*,¹³ which acknowledges employee safety, quality control, public image and workplace decorum as possible "special circumstances," demonstrating the applicability of the special circumstances exception will be challenging for employers. This is apparent from the *Tesla* decision, wherein the Board rejected

7 See, e.g., Ahiza García-Hodges, *Biden's vow to be 'most pro-union president' tested in first year*, NBC News (Jan. 20, 2022), <https://www.nbcnews.com/business/economy/bidens-vow-union-president-tested-first-year-rcna12791>.

8 See Ian Kullgren & Josh Eidelson, *Biden Fires NLRB General Counsel After He Refuses to Resign* (3), Bloomberg Law (Jan. 20, 2021), <https://news.bloomberglaw.com/daily-labor-report/biden-moves-to-oust-top-labor-board-attorney-robb>.

9 See The White House, *President Biden Announces Key Nomination on Jobs Team*, WhiteHouse.gov (Feb. 17, 2021), <https://www.whitehouse.gov/briefing-room/statements-releases/2021/02/17/president-biden-announces-key-nomination-on-jobs-team/>.

10 NLRB, *General Counsel Memorandum, The Right to Refrain from Captive Audience and other Mandatory Meetings*, NLRB Memo GC 22-04, nlr.gov (Apr. 7, 2022), <https://apps.nlr.gov/link/document.aspx/09031d458372316b>.

11 371 NLRB No. 131 (Aug. 29, 2022).

12 *Id.*; see also NLRB, *Board Rules Workplace Policies Limiting Wearing Union Insignia, including Union Apparel, are Unlawful Absent Special Circumstances*, nlr.gov (Aug. 29, 2022), <https://www.nlr.gov/news-outreach/news-story/board-rules-workplace-policies-limiting-wearing-union-insignia-including>.

13 342 NLRB 649 (2004).

Tesla's rule banning employees from wearing metal buttons because they could scratch and/or otherwise damage the cars.

The Tesla plant at issue was not unionized, and thus employers should be mindful that this decision, and the NLRA, impacts both union and nonunion employees equally. Employers with written dress code policies, particularly retailers with public-facing employees, should conduct a thorough review of any such policies.

The Rise in Strikes

With 2021 seeing a wave of strikes, it might be surprising to learn that, through the first half of 2022, there were three times as many US workers who went on strike than in the first half of 2021.¹⁴ According to Cornell University's labor tracker,¹⁵ between January and June of 2022, there were 180 strikes across the United States and its territories involving 78,000 workers, compared to 102 strikes involving 26,500 workers in the first half of 2021.¹⁶

2023 Expectations

With inflation and employee satisfaction showing no signs of returning to pre-pandemic levels, and the newfound fear of a looming recession (and, with it, the heightened fear of job loss and/or slashed wages), retailers should expect labor organizing to remain at the forefront of workers' minds and brace for this unionizing trend to continue through 2023.



Amber Rogers, Bob Dumbacher, Kurt Larkin and Crawford LeBouef
Amber, Bob and Kurt are partners, and Crawford is an associate, on the labor and employment team in the firm's Dallas, Atlanta, Richmond and Houston offices, respectively.

¹⁴ See Rani Molla, *How Unions Are Winning Again*, In 4 Charts, vox.com (Aug. 30, 2022), <https://www.vox.com/recode/2022/8/30/23326654/2022-union-charts-elections-wins-strikes>.

¹⁵ Cornell, *ILR Labor Action Tracker*, <https://striketracker.ilr.cornell.edu/> (last visited Nov. 29, 2022).

¹⁶ See Matthew A. Fontana, *Be Prepared: Important Trends for Employers to Know in Post-COVID Union Era*, Law.com (Oct. 25, 2022), <https://www.law.com/thelegalintelligencer/2022/10/25/be-prepared-important-trends-for-employers-to-know-in-post-covid-union-era/>; see also Sharon Zhang, *Workers Have Held More Strikes So Far in 2022 Than in All of 2021*, Data Finds, truthout.org (Oct. 3, 2022), <https://truthout.org/articles/workers-have-held-more-strikes-so-far-in-2022-than-in-all-of-2021-data-finds/>; see, further, Jason Lalljee & Juliana Kaplan, *Workers Are Getting Bolder. The Number of Strikes Tripled From Last Year as Americans See Their Wages Shrink and Bosses Profit*, Bus. Insider (Sep. 17, 2022), <https://www.businessinsider.com/more-workers-striking-unionizing-inflation-shortage-rail-biden-amazon-starbucks-2022-9#:~:text=In%20short%2C%20more%20workers%20have,and%20unfair%20labor%20practice%20charges.>



2022 Marks a Large Step Forward for ESG Disclosure

A global mandatory reporting regime for climate metrics and other ESG (environmental, social, governance) topics began to take shape in 2022. Two key developments drove this progression. First, in the United States, the Securities and Exchange Commission (SEC) proposed mandatory climate disclosures for public companies listed in the United States. Second, the European Union finalized the broad contours for a mandatory climate and ESG reporting regime for businesses—irrespective of whether they have a public listing—that conduct significant business in Europe. For retailers and consumer product companies with operations in the United States or Europe, these rules represent a sea change in ESG disclosure.

United States

On March 21, 2022, the SEC published a much-anticipated proposal to require that public companies disclose climate-related information. The [proposed rule](#) is significant because, for the first time, the SEC would mandate that companies (including foreign companies) publicly traded in the United States disclose climate-related risk and greenhouse gas (GHG) emissions information beyond the information currently required by existing SEC rules. As a proposal, the proposed rule is subject to a public comment period, and the SEC must vote a second time to adopt any final, binding rules. Nevertheless, it is clear the die has been cast.

Active with major organizations supporting retail industry, including the Retail Industry Leaders Association, the National Retail Federation and the Women in Retail Leadership Circle

Summary of the SEC Proposal

The SEC's proposed rule would define "climate-related metrics" and impose related governance, risk management, attestation, and strategy, business model and outlook disclosure requirements, among others. In brief, the proposal is aimed at requiring companies to disclose how they integrate climate risks and opportunities into their governance and corporate strategy along with a significant amount of related qualitative and quantitative information, including financial statement disclosure.

Governance: Public companies would be required to describe the board of directors' oversight of climate-related risks and, where applicable, climate-related opportunities. Core board oversight elements include:

- the identity of board members or committees responsible for oversight of climate-related risks;
- identification of board member expertise in such risks, with disclosure to "fully describe the nature of the expertise";
- processes for board evaluation of climate risks as part of the business strategy, risk management and financial oversight; and
- whether there are targets or goals, and how those are monitored and evaluated.

With respect to opportunities related to climate, if applicable, the proposed rule states that the company may describe its board oversight of these matters.

Strategy, Business Model and Outlook:

Public companies would be required to describe climate-related risks "reasonably likely" to have a "material impact" on the company, including on its business or consolidated financial statements, which may manifest over the short, medium and long term. Again, the SEC proposes that the company may also disclose such information about opportunities. The proposal then categorizes and dictates the types of risks and how they are to be disclosed and discussed, together with characterizations of the short-, medium- and long-term horizons, as well as impacts on useful life of assets, including:

- physical risks (like flooding), whether such risks are acute or chronic, and location and nature of properties, processes and operations subject to such physical risks, and
- transition risks (e.g., changing regulatory, technological or market regimes).

The company must then evaluate these impacts on the company strategy, business model and outlook. And, if adopted, the company must discuss whether such impacts, so described, are part of business strategy, financial planning and capital allocation. This process would include both current and forward-looking disclosures that "facilitate an understanding of whether the implications" of the risks identified are integrated into the business model or strategy and how the climate-related metrics, as defined, and the company's targets relate to the business's model or strategy. Furthermore, companies would be required to provide a narrative discussion of how the climate-related risks and metrics are reasonably likely to affect financial statements and whether they have had a material impact on reported financial conditions or operations. For companies that

maintain an internal carbon price, information on the pricing must be disclosed, including the rationale for deriving it. Finally, companies would be required to "describe the resilience of the business strategy in light of potential future changes in climate-related risks," and scenario analyses must be disclosed (with the SEC including as examples 3 C, 2 C, 1.5 C scenarios).

Risk Management: Companies would be required to describe any processes the company has for identifying, assessing and managing climate-related risks. If applicable, a company may also describe any processes for identifying, assessing and managing climate-related opportunities when responding to any of the provisions in this section. Key in this section are requirements to describe "any processes" for identifying and assessing climate-related risks, and to disclose how the relative significance of climate-related risks compared to other risks was determined and to consider "existing or likely regulatory requirements or policies," "shifts in customer or counterparty preferences, technological changes, or changes in market prices in assessing potential transition risks" and "materiality" of climate-related risks. Companies must also describe their process for how to decide whether to mitigate, accept or adapt to a particular risk, prioritize whether to address climate-related risks and determine how to mitigate any "high priority" risks, among other things.

GHG Emission Metrics and Attestation:

The SEC would require disclosure of GHG emissions for the most recently completed fiscal year and for historical fiscal years in the consolidated financial statements. Under the SEC's vision, within four years of the rule's effectiveness, all companies publicly traded in the United States would be required to report,

and obtain third-party assurance on, their own direct GHG emissions (Scope 1) and the GHG emissions associated with their purchase of electricity and other energy sources (Scope 2). Moreover, most companies would also ultimately be required to report their indirect GHG emissions associated with their suppliers and customers (Scope 3).

Scope emission disclosures would require a description of the methodology, significant inputs and significant assumptions made in the calculations, including organizational boundaries, operational boundaries, calculation approach and calculation tools. The proposed rule allows for use of “reasonable estimates,” but only if the underlying assumptions and reasons are described. Moreover, companies would be required to disclose “to the extent material” any use of third-party data when

calculating GHG emissions. And, if methodology and assumptions change year over year, such changes must also be described.

The attestation provisions of the proposed rule address what level of assurance of the information from an independent third party is required. For large accelerated filers (generally companies with greater than \$700 million market capitalization) and accelerated filers (generally companies with between \$700 million and \$75 million market capitalization), there must be an attestation report in the applicable SEC filings covering Scope 1 and Scope 2 emissions disclosures. The attestation must at a minimum be at a “limited assurance level,” i.e., equivalent to the level of review applied to unaudited quarterly financial statements, through the third fiscal year after the compliance date. After that, it

must be at a “reasonable assurance level,” i.e., equivalent to the level of review applied to audited annual financial statements.

The attestation report from the independent third party must be titled “Climate-Related Disclosure” in a separate section of the SEC filing. Nonaccelerated filers (generally companies with below \$75 million market cap or that have been public for less than one year) and smaller reporting companies would not be required to provide attestation reports.

Targets and Goals: The SEC would require a company to disclose if it has set any targets or goals related to reduction of GHG emissions “or any other climate-related target or goal (e.g., regarding energy usage, water usage, conservation or ecosystem restoration, or revenues from low-carbon products).” This will implicate a host of previously generated reports and goals that

have rolled out from companies over the past several years in response to international meetings on climate change (e.g., COP26 or COP27). Where carbon offsets or renewable energy credits (RECs) have been used as part of a company’s plan to achieve targets or goals, the company will have to disclose the amount of carbon reduction represented by the offsets or the amount of generated renewable energy represented by the RECs, the source of such offsets or RECs, a description and location of underlying projects, any registries or other authentication of the offsets or RECs and the cost of same.

Financial Statement Disclosure

Requirements: Quantified impacts of climate-related events and transition activities on line items in consolidated financial statements and related expenditures will need to be disclosed, as well as disclosure of financial estimates and assumptions impacted by these events and activities. The quantitative and qualitative disclosures provided in response to this requirement would, unlike the other disclosures contemplated by the proposed rules, be included in the company’s financial statements and therefore would be subject to the same level of review and audit by the companies’ independent auditors as other information in the company’s financial statements.

Public Comment and Phase-In

The SEC’s original public comment period ended on June 17, 2022, but was subsequently extended to November 1, 2022, after the SEC discovered a software deficiency with its online comment portal that may have delayed the receipt of some public comments. The proposed rule has received thousands of written comment letters, with commenters



advocating positions across a broad spectrum from total support to total objection to the proposed rule, and every point in between. Commenters submitted hundreds of highly technical letters analyzing the costs, benefits and challenges associated with the proposal, each of which the SEC must analyze and address before it can finalize any permanent rule. We anticipate that the SEC will take action to adopt a final, binding version of the proposed rule in the first half of 2023, though whether the agency chooses to adopt the full set of proposals or just some subset remains to be seen. Various commenters have threatened to challenge any final rules in court, which could further delay the timeline for implementation of any final rule.

The proposed rule provides for phased-in compliance with the largest public companies—large accelerated filers—subject to compliance as early as 2023 over a subset of the proposed rule, and then through 2027 additional compliance and disclosure obligations would begin to take effect each year. Mid-size and smaller public companies would have more time to come into compliance and would have slightly fewer obligations. It is quite possible the timeline for compliance will slip a year or more in any final rules, depending on when the SEC finalizes rules and the outcome of any follow-on litigation challenging them.

Client Resource

Hunton Retail Law Resource

Written by members of our firm’s experienced team of lawyers who serve retailers from factory floor, to retail outlet, to online store, the Hunton Retail Law Resource Blog helps you stay abreast of the legal and regulatory issues facing your company and helps you minimize risk in this highly competitive and ever-changing industry. With a regular digest of breaking legal news and information delivered to your desktop, our blog reports cover topics including corporate law, FTC and SEC consumer protection and antitrust matters, labor law, litigation, retail class actions, and privacy and cybersecurity.

[Subscribe now](#) to Hunton Retail Law Resource Blog for the latest legal updates, developments and business trends that affect your retail business.

European Union

On November 28, 2022, the Council of the European Union (EU) formally adopted the Corporate Sustainability Reporting Directive (CSRD), following the European Parliament's formal adoption of the directive earlier last month. The CSRD is a broad ESG reporting framework that will impose uniform, mandatory reporting requirements on many companies with European operations, including companies not based in Europe, and without regard to whether they have a public listing on a European stock exchange.

The CSRD is not the first corporate ESG reporting regime in the EU; the Non-financial Reporting Directive (NFRD) has been in effect since 2018 and has required disclosures across ESG pillars. But the CSRD, which replaces the NFRD, represents a step-change in mandatory ESG reporting nonetheless. And the CSRD is just one component of the EU's sustainable finance framework, which also includes ESG disclosure requirements for financial market participants with the Sustainable Finance Disclosure Regulation (SFDR), and the EU Taxonomy Regulation, a system requiring both companies and financial market participants to classify their "sustainable" economic activities under defined criteria.

The scope of entities subject to the CSRD is far greater than under the NFRD. An estimated 12,000 European companies are subject to the NFRD, representing only the largest, so-called "public interest" entities—primarily companies with securities listed on EU-regulated markets, banks and insurance companies with 500 or more employees. By contrast, the European Commission estimates that roughly 50,000 companies will fall under the CSRD's reporting obligations. In addition to those companies currently subject to the NFRD, this will include:

- all "listed" companies offering securities on an EU index (except for "micro-enterprises");
- all "large" companies, meaning those that meet at least two of three criteria: (i) a balance sheet of €20 million, (ii) net turnover of €40 million and (iii) 250 employees or more on average during the year—parent undertakings of "large groups" that meet two of these criteria on a consolidated basis also qualify; and
- non-EU companies, so-called "third-country undertakings," with significant European operations—i.e., that generate a net turnover of €150 million or more in the EU and that have an EU subsidiary that is either listed on an EU-regulated index or "large" under the above criteria, or an EU branch generating an annual net turnover of €40 million in the prior year.

The breadth of these categories means that the CSRD will have impacts on companies based in the United States and elsewhere, provided they have European operations above the established thresholds. The CSRD provides for an exemption for the EU subsidiaries or branches of a non-EU parent if the EU operation was included in the parent undertaking's consolidated management report that had sustainability disclosures deemed to be "equivalent" to those required under the CSRD. But, because the process for determining equivalence is as yet unclear, there is considerable uncertainty as to how this may apply in practice. For US companies, there is further skepticism that the far more limited scope of the SEC climate change disclosure proposal, which, if finalized, would address only climate-related disclosures, would be deemed equivalent to the CSRD. Other pending or expected SEC rule proposals on matters such as cybersecurity and human capital would not necessarily bridge this gap.

Several other elements of the CSRD are also of particular note:

Uniform Reporting Standards. The CSRD will impose uniform, comprehensive reporting standards applicable across the EU, under forthcoming European Sustainability Reporting Standards (ESRS). The ESRS will call for disclosures of numerous metrics across the ESG pillars, including things like energy and emissions data, water use, climate-related risk management strategies, circular economy, pollution, biodiversity under the "E"; working conditions, diversity, inclusion, human rights under the "S"; and business risk, strategy and board oversight over sustainability information under the "G." The ESRS are still under development by the European Financial Reporting Advisory Group (EFRAG).

Double Materiality. Under the CSRD, subject companies must report according to a "double materiality" perspective, wherein they must consider not just the material impacts of ESG factors to the organization but also the organization's own impacts on the environment and social systems. This is distinct from the SEC's climate reporting proposed rule, which embraces a "single materiality" perspective that would require disclosure of only climate-related impacts to the reporting entity.

Third-Party Assurance. The CSRD will impose a third-party assurance, or audit, obligation on reporting entities, requiring reporting to be certified by an accredited independent auditor. Only "limited" assurance will be required to start. Subsequently, however, the CSRD provides for development of a more rigorous, "reasonable" assurance standard in 2028, if it is found to be feasible.

Reporting Mechanics. The CSRD requires that companies report ESG metrics not in a separate sustainability report but in a dedicated section of the broader company management report, thus blending the sustainability and other financial reporting into a single document. Companies also must digitally tag sustainability information to allow the EU to maintain a singular, uniform database of CSRD disclosures, furthering the goal of increasing transparency and accessibility of sustainability disclosures.

The CSRD takes a phased approach to implementation, with different categories of companies becoming subject to the reporting requirements along a staggered timeline. Large "public interest" undertakings already subject to the NFRD and large listed companies with 500 or more employees will be subject starting January 1, 2024; "large"





Next Steps

The CSRD requirements and those proposed by the SEC are based to some degree on preexisting voluntary guidelines and standards (including the recommendations of the [Task Force on Climate-Related Financial Disclosures \(TCFD\)](#) and the [Greenhouse Gas Protocol](#)). While some retailers have partially relied on these guidelines and standards to prepare and publish climate-related disclosures in the past, those companies have still exercised discretion as to what disclosures they have made and their content. Moreover, those disclosures have not necessarily been subject to the level of comprehensive, prescriptive rigor contemplated by the SEC or the EU.

to report. An official submittal to the SEC, for example, is subject to greater internal and public scrutiny in all respects, as well as additional potential liability under US federal securities laws. Collectively, the new EU and SEC rules will require creation of a compliance infrastructure that will involve in-house environmental professionals, outside consultants, in-house and outside environmental and governance lawyers, internal audit systems and third-party independent attestation firms, just to name a few.

A particular challenge that the EU and SEC rules present is that both have degrees of extraterritorial effect, and both have been prepared in parallel without a high level of coordination across the Atlantic. Overlap between the two regimes is more coincidental than intentional. In particular, European rules were not drafted with a view toward the litigation environment in the United States, which will impose on retailers reporting in Europe the added burden of ensuring that European disclosures do not become a source

of liability to American plaintiffs. Conversely, the SEC's proposal was not prepared with an eye toward satisfying the more stringent European disclosure obligations, such that retailers with operations on both sides of the Atlantic may eventually be subject to two very different mandatory ESG reporting regimes.

At this point, European retailers and non-EU companies with European operations should begin the complex evaluation process to determine whether and when they will be subject to the CSRD and its reporting obligations. Retailers publicly listed in the United States should take care to ensure that any future European disclosures are consistent with their SEC filings and other public disclosures made in the United States. Retailers with US operations should craft disclosures under the CSRD with due regard to the growing body of regulations and caselaw in the United States concerning greenwashing. Then, this exercise should be repeated for publicly traded retailers when the SEC finalizes its rules.

undertakings not currently subject to the NFRD will be subject beginning January 1, 2025; and "small and medium-sized undertakings" with securities listed on an EU-regulated market, as well as small and noncomplex credit institutions and captive insurance undertakings, will become subject January 1, 2026. Non-EU companies subject to the CSRD must comply beginning January 1, 2028. For all of these groups, initial reports under the CSRD would be required to be produced the following year.

Now that it has been formally approved, the CSRD will be signed and published in the Official Journal of the EU and will enter into force 20 days later. EU member states will then have 18 months to transpose the CSRD into their respective national laws. More details on exactly what the mandatory reporting standards will look like will become clear over the coming months, as the EU considers and adopts a delegated act setting forth ESRS by June 30, 2023, and a second, sector-specific set of ESRS by June 30, 2024.

The new CSRD requirements, along with any new rules the SEC adopts, are likely to require even the most dedicated and well-resourced retailers to expand and enhance their ESG reporting. For the many companies that have just begun their ESG reporting journey on a voluntary basis, the undertaking will be even more substantial.

The elevation of the directive to disclose climate information to a regulatory requirement also changes the work that companies will practically need to undertake



Scott Kimpel, Shannon Broome, Sam Brown, Sam Kardon and Alexandra Hamilton

Scott is a partner in the capital markets practice, heads Hunton's ESG practice and also leads the firm's working group on blockchain and digital assets in the firm's Washington, DC office. Shannon is the managing partner of the firm's San Francisco office and leads the California environmental practice. Sam is a partner on the environmental team in the San Francisco office. Sam is counsel in the capital markets practice in the New York office. Alexandra is an associate on the environmental team in the San Francisco office.

Key Contacts



Robert Quackenboss

Partner, Washington, DC
+1 202 955 1950 | rquackenboss@HuntonAK.com

Bob is the editor of the 2022 Retail Industry Year in Review. He represents businesses in resolving their complex labor, employment, trade secret, non-compete and related commercial disputes.



Steve Patterson

Partner, Washington, DC
+1 202 419 2101 | spatterson@HuntonAK.com

Steve is co-head of the firm's mergers and acquisitions group, co-chair of its retail and consumer products industry group and serves on the firm's executive committee. His practice focuses on public and private securities offerings, securities compliance, mergers and acquisitions and corporate governance matters.



Ryan Phair

Partner, Washington, DC
+1 202 955 1921 | rphair@HuntonAK.com

Ryan is co-chair of the firm's antitrust and consumer protection practice and co-chair of the firm's retail and consumer products industry group. He is an experienced trial lawyer who works extensively with myriad retailers, often on a daily basis as national coordinating counsel, to address litigation risks and related issues.

About Us

Hunton Andrews Kurth is a global law firm of more than 900 lawyers handling transactional, litigation and regulatory matters for clients in myriad industries including retail and consumer products, energy, financial services, real estate and technology. Areas of practice focus include capital markets, mergers and acquisitions, intellectual property, P3, public finance and infrastructure, and privacy and cybersecurity. With offices across the United States and in Europe, the Middle East and Asia, we're aligned with our clients' businesses and committed to delivering exceptional service.

Our retail industry lawyers represent businesses at every step, from factory floor, to retail outlet, to online store. Our extensive list of international, national and regional clients includes many well-known restaurant chains, malls, home-improvement centers, supermarkets, and media and entertainment companies, as well as manufacturers and retailers of apparel, baby products, cosmetics, electronics, fine jewelry, luxury goods, toys and other merchandise. Our retail team is composed of more than 300 lawyers who represent retailers in the Fortune 500® and virtually every retail sector.

Please visit [HuntonAK.com](https://www.huntonak.com) for more information on our industries and practices.



Scan Code
to get this brochure on your smartphone

© 2023 Hunton Andrews Kurth LLP. Attorney advertising materials. Hunton Andrews Kurth, the Hunton Andrews Kurth logo, HuntonAK and the HuntonAK logo are service marks of Hunton Andrews Kurth LLP. These materials have been prepared for informational purposes only and are not legal advice. This information is not intended to create (and receipt of it does not constitute) an attorney-client or similar relationship. Please do not send us confidential information. Past successes cannot be an assurance of future success. Whether you need legal services and which lawyer you select are important decisions that should not be based solely upon these materials. Photographs are for dramatization purposes only and may include models. Likenesses do not necessarily imply current client, partnership or employee status. Hunton Andrews Kurth LLP is a Virginia limited liability partnership. Contact: Walfrido J. Martinez, Managing Partner, Hunton Andrews Kurth LLP, 2200 Pennsylvania Avenue, NW, Washington, DC, 202.955.1500.