RETAIL INDUSTRY

YEAR IN REVIEW

2023

HUNTON
ANDREWS KURTH

Published January 2024

TABLE OF CONTENTS

California Attorney General Issues Stark Warning to Businesses Regarding Enforcement of Ingredient Disclosure Laws and Bans Food Packaging and Cookware Containing PFAS Sold in California 4

Retail Employers Face New Challenges From Pro-Labor Measures Implemented by Biden NLRB in 2023 7

Policing Your Brand on Online Marketplaces: A Brief IP Overview for Retailers 11

Are You Covered?: Social Media Exposure for Retailers 14

Blazed and Confused: Balancing Workplace Safety with Expanded State Law Employment Protections for Cannabis Use 18

SEC Cybersecurity Disclosure Rules Take Effect 22

2023 Litigation Trends for PFAS-Containing Consumer Products and 2024 Preview 27

EEOC Issues New AI Guidance in 2023 30

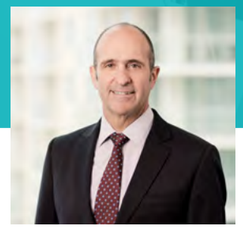
Key Legal Issues in Data Breach Litigation 32

Washington, Nevada and Connecticut Enact Health Privacy Laws 35

Legal Considerations for Corporate Circular Economy Strategies 38

Key Contacts 41

About Us 42



Dear Clients and Friends,

Look up the dictionary definition of "retail," and you will find something along the lines of "the sale of goods in small quantities to consumers." But we all know retail goes far beyond that, touching the economy and consumer life in countless ways and uniting diverse legal practice areas.

We see it in our own work every day. In 2023, Hunton Andrews Kurth LLP's *Chambers USA*'s honored retail industry team partnered with our retail clients to tackle matters ranging from cyber incidents, to lease negotiation, to trademark infringement, to personal injury litigation, to environmental contamination, and so much more.

Our *2023 Retail Industry Year in Review* explores retail issues and developments we observed throughout the past year—in your matters, in legal opinions and regulation, and in the news—and a glimpse into what we expect in 2024. As just a few examples:

- Our ALG team takes a look at PFAS regulation regarding food packaging and cookware in California;
- Our litigation team sets forth the latest trends in data breach class actions against retailers;
- Our labor and employment team examines state drug laws and OSHA obligations; and
- Our insurance team addresses coverage for social media-related copyright infringement cases against retailers.

I hope that the analysis in this *2023 Retail Industry Year in Review* serves as a practical guide in approaching retail-related concerns that are critical to your business. As always, we look forward to confronting new retail challenges with you head-on and supporting you in the year to come.

Sam

Samuel A. Danon
Managing Partner

California Attorney General Issues Stark Warning to Businesses Regarding Enforcement of Ingredient Disclosure Laws and Bans Food Packaging and Cookware Containing PFAS Sold in California

On October 17, 2023, the California Attorney General (AG) Rob Bonta released an enforcement advisory letter to manufacturers, distributors and sellers of food packaging and cookware detailing how he intends to enforce AB 1200, a law that: 1) bans the sale of regulated per- and polyfluoroalkyl substances (PFAS) in food packaging in California and 2) requires disclosure and labeling of chemicals on a "designated list," including PFAS, that are present in the food contact surface or the handle of cookware products sold in California.

Because the individual laws do not provide specific enforcement mechanisms, this announcement is the first time the AG's office has articulated the authorities it plans to use to enforce these laws. The enforcement advisory letter provides a clear warning to the regulated community, from manufacturers to importers to distributors and retailers, that California will be enforcing its PFAS laws. Similar advisories could be issued in the future for California's other laws restricting the sale of juvenile products, textiles and cosmetics containing PFAS.

AB 1200: Chemicals in Food Packaging and Cookware

Since January 1, 2023, no person can legally distribute, sell or offer for sale in California any food packaging that contains regulated PFAS. Regulated PFAS includes either PFAS that are intentionally added or PFAS in a product or product component at or above 100 parts per million (ppm), as measured by total organic fluorine. Manufacturers must also use the least toxic alternative when replacing regulated PFAS in food packaging. Food packaging is defined broadly as nondurable packaging, packaging components and food service ware that is "comprised, in substantial part, of paper, paperboard, or other materials originally derived from plant fibers."

Additionally, manufacturers of cookware must comply with website disclosure requirements (which went into effect January 1, 2023) and labeling requirements (which went into effect January 1, 2024) for cookware products sold in California where the handle or food contact surface of the cookware contains one or more chemicals on the Department of Toxic Substances Control (DTSC)'s "designated list" is intentionally added in. The "designated list" of chemicals includes "PFAS" as a class, along with 3,297 other chemical substances that DTSC has identified as candidate chemicals that exhibit a hazard trait or an environmental or toxicological endpoint.

AB 1200 also prohibits manufacturers from making claims that cookware is free of any specific chemical if the chemical belongs to a chemical group or class identified on the "designated list" unless no individual chemical from that chemical group or class is intentionally added to the cookware. For example, a product cannot claim to be PFAS-free if it contains any type of PFAS in the product.

California Attorney General's Enforcement Advisory Letter

The AG's enforcement advisory letter informs manufacturers, distributors and sellers (including retailers) of food packaging and cookware of new requirements established under AB 1200. Prior to issuing this letter, it was unclear to the regulated community how the state of

California would enforce its PFAS laws, without specific enforcement authority provided in the statutes themselves. The AG's letter now clarifies that failure to comply with these laws may constitute a violation of California's Unfair Competition Law, Business and Professions Code section 17200 (UCL), Business and Professions Code section 17500 and other applicable laws. The AG warns that his office may bring an enforcement action seeking civil penalties, restitution, injunctive relief or even criminal liability for failure to comply with AB 1200. Civil penalties for BPC violations can be up to $2,500 per violation (arguably, per product sold in California).

Under limited circumstances, in addition to the AG enforcement, private parties can also bring claims for non-compliance with PFAS laws based on the UCL.

Tracking State PFAS Restrictions

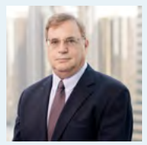
States like California have been active in the past few years passing laws to regulate PFAS in products. So far, 12 states have enacted laws that ban or impose reporting or disclosure requirements for PFAS in products ranging from food packaging to textiles to cosmetics, cookware to juvenile products to carpets, rugs and upholstered furniture.

While each state's requirements differ to some extent, states have uniformly adopted the same sweeping definition of PFAS: a class of fluorinated organic chemicals containing at least one fully fluorinated carbon atom. Additionally, no state has established any de minimis level or thresholds for intentionally added PFAS.

As states continue to move forward with emerging PFAS product restrictions, those who manufacture, distribute and sell such products must prepare for the changing legal landscape. Six states have PFAS requirement deadlines in 2024 and eight have deadlines in 2025. Minnesota and Washington have deadlines in 2026; Colorado and Oregon have deadlines in 2027; Maine has deadlines in 2030; and Minnesota has deadlines in 2032.

The sheer scope of these state laws has subjected potentially millions of products currently sold or distributed in states to various labeling, disclosure and reporting requirements or bans. This trend creates challenges for product manufacturers and retailers alike. Companies have to ascertain which of their products are impacted, where those products are impacted and how to gather the information they need to determine if even trace amounts of PFAS are in their products or in the materials used to manufacture their products.

The Hunton Andrews Kurth PFAS in Products State Law Tracker is a publicly accessible tool to help companies track state statutes and regulations that ban or impose reporting or disclosure requirements for products containing PFAS. As state requirements for products containing PFAS continue to emerge, companies will need to regularly track these developments and prepare to assess the presence of PFAS in their supply chains. Businesses should also review each state's laws and consult knowledgeable counsel to understand the nuances of each law. Because these laws are fast-changing and developing, it is incumbent on businesses to stay current as more laws change and new ones are adopted.



Malcolm Weiss, Javaneh Tarter and Jaclyn Lee

Malcolm is a partner and Javaneh is a senior attorney on the environmental team in the firm's Los Angeles and Washington, DC offices, respectively. Jaclyn is a law clerk on the environmental team in the firm's Washington, DC office.

Retail Employers Face New Challenges From Pro-Labor Measures Implemented by Biden NLRB in 2023

In 2023, the Biden National Labor Relations Board (NLRB or Board) and its General Counsel Jennifer Abruzzo continued implementing a highly pro-labor agenda that has significantly changed the union and labor landscape for retail employers. In addition, Abruzzo and the Board's Regional Directors are imposing and enforcing aggressively some of their most controversial new measures against prominent retail employers to create and affirm new precedent, easing that path for union representation nationwide.

The Acceleration in Retail Union Organizing

2023 opened as union organizing efforts, including within retail, were already accelerating. Buoyed by the pro-labor agenda and rulemaking by the Biden Board, 2022 saw a 53 percent increase in the number of election petitions filed over 2021. This was the highest number of union representation petitions filed since 2016. The surge in retail organizing has seen traditional national unions such as the UFCW, Teamsters and others focus on grocery chains, retail stores, cannabis dispensaries, pharmacies and online retail companies, with a focus on strategic labor strikes that impact retail customer satisfaction.

And while unions historically have avoided organizing individual retail stores (preferring the larger targets of regional, warehouse and supply chain workforces), the emergence of so-called "homegrown" unions, purportedly unaffiliated with the large national unions, changed that over the past several years. Grassroots unions such as Starbucks Workers United,

the REI Union, Trader Joe's United, Pharmacy Workers United and Apple Retail Union, among others, have changed the calculus for both organizers and employers by attempting to organize and seek representation at the single-store level. As a result, employers and franchises are on heightened alert for piecemeal organizing that has previously presented a very limited challenge.

Notably, even retail employers boasting progressive company cultures and higher wages are not immune to the trend. The growing Gen Z and Millennial workforces still seek union representation at such employers, motivated by social justice issues, work-life balance and safety issues more so than the traditional economic motivators (wage and benefits) of union organizing.

2023 Developments That Ease the Path to Union Representation

The Board took several steps this year to further ease the path to union representation, all of which increased the special challenges for retail employers. First, the Board's August 25 decision in *Cemex Construction Materials Pacific, LLC* changed dramatically the historic and balanced process by which the Board determines whether an employer must recognize a union as representative of a bargaining unit. Cemex now establishes that the traditional process for which unions obtain certification—filing a petition for a secret ballot election, and allowing the employer to campaign against union representation—may be bypassed by unions that merely make a written demand for representation. Doing so now effectively shifts the burden of seeking an election from the union to the employer. In response to such a demand, the employer must now either agree to recognize the union or bear the burden of filing an "RM" election petition of its own within two weeks of receiving the demand. Otherwise, the employer risks the union being installed without an election, and perhaps without any meaningful test of whether employees truly desire union representation.

Cemex went even further by clarifying that employers that challenge the union's demand by seeking an election bear heightened risks in doing so: should the employer engage in conduct that would require setting aside the election (which is often low-level ULPs) in the course of that campaign, the Board has new freedom to order a *Gissel*-style bargaining order and overturn the election results altogether. Cemex currently is under appeal and the outcome of that appeal may be known in 2024.

The Biden Board further complicated an employer's ability to resist union representation by resuscitating the Obama Board's 2014 "ambush" election rules. Like the 2014 rules (which were withdrawn under the Trump administration) the Biden Board's 2023 rules significantly shorten the time between when a representation petition is filed and the election itself. The employer's deadlines and timeframes for important filings are similarly shortened. This condensed pace makes it challenging for employers to educate voters about unionization prior to the vote. The likely result of the return to this rule will be the negative effect on employees who may not have enough time to fully consider their vote.

The *Cemex* decision and the return to ambush election rules together undermined the employer's traditional ability to respond to union organizing coherently, cautiously and with open and effective communication. For retail employers, those disadvantages are magnified because of the new and unorthodox tactics already in play from the homegrown unions, their focus on smaller and younger workforces, and the array of new tactics and motivations driving the efforts.

New Joint Employer Rule Heightens Risk for Retailers and Franchisors

In October 2023, the Board published its anticipated Final Rule regarding joint-employer status, relaxing the standard by which an entity may be considered a joint-employer with another entity. Under the prior rules, an entity was considered a joint-employer only if it exercised "actual *and direct control*" over an essential term of employment. Under the new rule, merely "*actual or indirect* control" of one or more employees' essential terms of employment will establish a joint employer relationship. The proposed new rule will have a significant impact on retail employers that separate operations among companies that employ distinct employee groups serving different brands or product categories. Under the new rule, liability for collective bargaining obligations, ULP and other labor law liability could attach to separate entities, third-party contractors and across franchisee-franchisor relationships. Legal challenges have been raised to the new rule, causing the Board to postpone the effective date of the new rule to February 26, 2024.

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.


HUNTON ANDREWS KURTH

OCTOBER 2023

Hot Topics for Retail General Counsel

Stericycle Handbook Policy Ruling Stings Retailers

In August, the Board imposed a more permissive standard to judge if a handbook policy is unlawful for chilling an employee's exercise of Section 7 rights (to engage in concerted activities for the purpose of collective bargaining or other mutual aid or protection). The prior standard looked at "the nature and extent of the potential impact on NLRA rights" and an employer's "legitimate justifications associated with the rule." In its August *Stericycle* decision, the Board relaxed the standard, removing the employer's intent from the analysis and making a policy "presumptively unlawful" if an employee could "reasonably interpret" a policy as restricting Section 7 rights.

The new standard creates an outsize burden on retailers, who often rely heavily on conduct-based policies for employees who interact with customers. For example, policies addressing workplace civility, profanity, confidentiality, personal email and phone use, workplace attire and union insignia, and solicitation all will be scrutinized under this subjective new standard.

Campaign to Restrict Retail Employer Free Speech

2023 also saw the continued effort by the Biden Board to restrict both the logistics and content of employer speech to employees about unions and representation. In April 2022, NLRB General Counsel Abruzzo stated her intention to seek Board prohibition of so-called "captive audience meetings" during union election campaigns. Abruzzo's position is that such mandatory meetings, which are sometimes a retail employer's only opportunity for direct communication with employees about the facts of union representation, are unlawful. In 2023, Abruzzo pursued a litigation strategy to achieve that goal, filing complaints against high-profile employers such as Amazon for using employee meetings to speak with employees about their rights under the NLRA.

Abruzzo has also accelerated litigation over alleged ULPs based on claims of employer speech violations. One such action is against Starbucks and Starbucks's CEO Howard Schulz for allegedly unlawful speech for stating during a public earnings call "[w]e do not have the same freedom to make these improvements at locations that have a union or where union organizing is underway" in the context of wage raises to US-based employees. The General Counsel argued that Schultz's comments interfered with employees' rights to organize.

Conclusion

While litigation and appeals play out in 2024, retail employers should confer with counsel about their readiness to adapt to the new labor landscape rolled out in 2023. Retail employers should prepare for homegrown union activity at single-store locations, readiness for reacting to new election rules and a *Cemex* demand for representation. They should review multi-entity business models for exposure under new joint-employer rules, along with handbook policies and communication protocols to assess risk.

Robert Quackenboss

Bob is a partner on the labor and employment team in the firm's Washington, DC and New York offices. He is the editor of the 2023 Retail Industry Year in Review.

Policing Your Brand on Online Marketplaces: A Brief IP Overview for Retailers

Retailers often face brand policing challenges on online resale platforms such as Wayfair, Overstock.com and eBay. Resellers account for a significant portion of retail sales on these websites. Resellers tend to be small to midsize entities but are nevertheless able to reach a large number of US consumers. It's thus unsurprising that problems arise daily, often relating to brand owners' dissatisfaction with the third-party resellers and their sales practices.

How can trademark and copyright laws help and what are the recent trends in this area?

The situation may arise, for example, where a product receives poor reviews, but the reviews are a result of the third-party seller's actions rather than the product itself, e.g., a product may arrive not as described in the reseller's listing. One approach to try to curtail poor product reviews stemming from a reseller's conduct and misrepresentations is to bring a false advertising claim against the third-party reseller based on the untrue or misleading product description statements.

Another example of a problem in this space is price gouging that can lead to overall consumer dissatisfaction. The ultimate harm stems from a perceived association between the brand owner and the third-party seller. In this scenario, a brand

owner may have a claim against the third-party reseller for false association. The theory is that the third-party seller is holding itself out as an agent of or authorized distributor for the brand owner or is otherwise approved by the brand owner.

Fake third-party reviews are another challenge. If a brand owner is a victim of this practice, it may bring a contributory false advertising claim against the party purchasing fake reviews. The theory is that the fake review purchaser is causing the online platform to falsely advertise the quality of the brand owner's product.

"Listing sabotage" is also a recurring issue. Some online platforms maintain product listings that third-party sellers may use for a given product. Because these listings are commonly maintained, images and descriptions relating to the product may be added by third parties. In some instances, competitors for a given product have uploaded misleading or incorrect images for a product listing. This results in consumer confusion, decreased sales, dissatisfied customers and reputational harm to the brand owner in the form of bad reviews. In some instances, copyright law may be leveraged to combat these anticompetitive practices.

Grey market products present a challenge on online platforms. Grey market products are not "fake," per se, but rather travel outside approved distribution channels. When third-party resellers offer these products for sale, the pricing may undercut a brand owner's pricing for the given distribution channel. Brand owners often attempt to deal with grey market products by refusing warranty on such products, but this does not mitigate reputational harm or address the underlying problem. In this instance, the brand owner may be able to argue that the lack of a warranty on grey market goods is a material difference from the normal product and, therefore, a trademark infringement claim may be asserted.

Lack of quality control is yet another challenge relating to online platforms. A brand owner that desires to prevent an unauthorized reseller on an online platform may consider whether there are established quality controls for the product at issue and whether a third-party reseller is abiding by those quality controls. If not, the brand may suffer. As such, the brand owner may allege that the reseller's product is materially different from the brand's own product and, therefore, the first sale doctrine does not apply. On that basis, the brand owner may allege trademark infringement.

Finally, while it may be hard to believe, brand owners are often recipients of false trademark infringement claims (or false IP claims in general) on online platforms every day. There are instances where a brand owner is lawfully selling its own products on an online platform but receives a false trademark (or other IP) infringement complaint. Bringing a declaratory judgment claim against the party alleging the infringement claim might help. Another approach is to bring a defamation claim against the alleging party.

In 2023, we observed a significant increase in the number of declaratory judgment actions filed against brand owners who submitted complaints on online platforms or even sent simple cease-and-desist letters. Many declaratory judgment plaintiffs are foreign-based entities that, in the past, did not participate in US-based intellectual property disputes. Similarly, the number of motions for preliminary injunction in trademark disputes increased. Both a declaratory judgment action and a motion for preliminary injunction raise the cost of litigation and tend to be more aggressive in nature than conventional approaches, e.g., settlement negotiation prior to running to the court, and place the issue immediately before a district court judge.

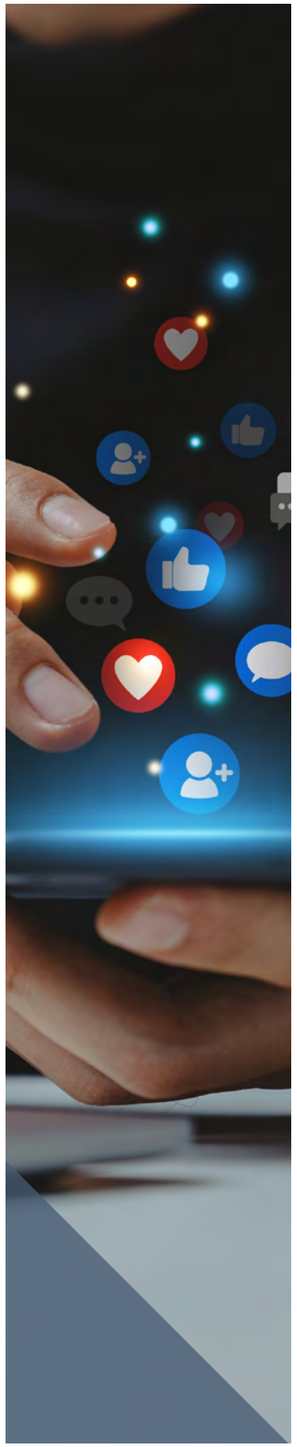
In short, while sale of branded products on online marketplaces presents challenges, trademark and copyright law may be used to attempt to curtail anticompetitive behaviors on the platforms. Accordingly, retailers are advised to take steps to adequately protect their intellectual property—such as registering their trademarks and copyrights to help facilitate swift action against third-party resellers, among other benefits—and continuously monitor online marketplaces for the practices described above. In view of recent developments, however, retailers are also advised to carefully consider enforcement strategies prior to blindly contacting an alleged infringer because of the trend in emboldened response behavior.

A longer version of this blog post originally appeared as an article in Retail TouchPoints: Policing Your Brand on Online Marketplaces: an Intellectual Property Guide for Retailers. Further duplication is not permitted.



Armin Ghiam, Jeremy Boczko and Matthew Nigriny

Armin and Jeremy are partners in the intellectual property practice in the firm's New York office, and Matthew is an associate in the intellectual property practice in the firm's Richmond office.



Are You Covered?: Social Media Exposure for Retailers

As the reliance on social media to promote a business's products or services has increased, so too have copyright infringement claims, making it more important than ever for retailers and those who facilitate their advertising campaigns to understand the intersection of copyright law and social media. Claims that were previously exclusive to publishers have now reached major retailers who market their products through the business's social media posts or third-party influencer posts. Nowadays, re-sharing photos, videos, music or other user-generated content without the user's permission can expose retailers to significant legal liability and risks. Being on the wrong side of a copyright infringement lawsuit could cost a retailer thousands, if not millions, of dollars in legal fees and damages. Fortunately, a comprehensive insurance program can help mitigate these expenses if a retailer is accused of unauthorized use of copyrighted works.

The Risks

Understanding the potential risks is crucial to recognizing the activities that can expose retailers to copyright infringement claims. For example, businesses that create and share photos and videos to promote their product or service can be subject to liability for copyright infringement should they choose to use content without approval from the creator.

In addition, retailers who use music on social media or on their website are also at risk. Copyright exposure arises if the music is not properly licensed, even if the music is playing innocently in the background. Nor is it a defense if the account has a low following. Likewise, crediting the original creator does not afford automatic protection, nor does it confer the right to use copyrighted work. Instead, linking to the source and giving attribution to the original creator notifies the creator of unauthorized use. There is also software that can detect inappropriate uses of copyright on the internet, which has contributed to the aggressive increase in claims.

Copyright infringement claims can expose retailers to high defense costs, actual damages, statutory damages and attorney's fees. Uploading or downloading copyrighted works without permission from the creator violates the creator's exclusive rights to reproduce and distribute. Those who commit copyright infringement may face federal statutory damages of up to $30,000 per work infringed. In cases of willful infringement, this amount can be raised to $150,000 per work.[1] This is significant because, as retailers seek to lean into trends such as short-form videos with music cues and elements on Facebook, Instagram or TikTok, so too are copyright infringement cases being brought against retailers for use of unlicensed music.

For example, a retailer known for its aggressive and flashy social media strategy that used popular influencers to advertise on TikTok and Instagram was hit with copyright lawsuits from all three of the major US record labels for failure to obtain a license to use the music in more than 100 of its videos. A federal judge ruled for the labels, finding the social media posts to be "work." In other cases, creators have elected for quicker alternatives such as sending retailers cease and desist letters along with settlement demands or bills for the creators' licensed work. These examples underscore the importance for retailers t o analyze their exposure to copyright infringement claims and develop a strategy to mitigate and decrease liability.

Mitigating the Risks and Potential Solutions

While there may not be an all-encompassing solution for retailers to avoid copyright infringement claims, retailers can minimize the potential impact of copyright infringement claims by relying on a comprehensive insurance program, having a clear social media governance policy and using original content.

Insurance is available to help mitigate risks from copyright infringement claims. Insurance is not a substitute for risk mitigation; rather, appropriate insurance should be *part of* a broader risk-mitigation plan. The role of insurance as a component of a broader risk-mitigation plan is twofold. First, as many would expect, insurance may help lessen or eliminate out-of-pocket loss should a copyright violation occur. Second, and often overlooked, insurance may help reduce or completely cover the cost of defending claims of copyright infringement, even if those claims don't result in liability. Indeed, it is often the case that the cost of defending a lawsuit can be worth more than paying the amount of any judgment or settlement that might result.

A good social media governance policy to ensure posts sharing music or content of others have been approved by the creator is also part of a broader risk-mitigation plan—one that most insurers will require retailers to have in place. This is especially important for retailers that contract with third-party influencers to market their products and services. The governance policy should account for security provisions, regulatory compliance requirements and copyright infringement prevention tactics such as specific guidelines around reposting

1 17 U.S. Code § 504 - Remedies for infringement: Damages and profits.

content, using trending sounds and partnering with third-party creators.

Creating original content for social media is another way to mitigate the risk of copyright infringement claims. While jumping on trends, such as trending music, and reposting content are powerful plays to increase social media engagement, their dangers might outweigh their benefits. If posting original content may not be ideal, because of costs or otherwise, retailers that use third-party content should make sure they, and any contracted third parties, understand the proper licensing and permissions that should be in place to avoid copyright violations.

Relevant Insurance Coverage

Adequate and appropriate insurance coverage can help safeguard copyright infringement claims should they arise. From media liability to commercial general liability (CGL) to cyber insurance, retailers can leverage insurance for defense costs, judgments or settlements related to copyright infringement claims. Every policy, however, includes unique language and defined policy terms. Retailers should carefully review their policies and consult insurance professionals to ensure there is adequate coverage for specific business risks.

Notably, most CGL policies do not explicitly cover intellectual property (IP) risks, such as copyright infringement claims. Typically, the policy will contain what is known as an intellectual property exclusion. The policy will include coverage for advertising injury, which aims to protect businesses from claims of offenses committed in advertising, including online platforms. But this coverage is often diluted by restrictive definitions and broad exclusions that might render coverage for copyright infringement illusory. Unlike trademark infringement claims, which, by their nature, involve advertising, the relationship between a copyright claim and advertising is not automatic. Further, the common policy phrase "in your advertisement," which is frequently used in standard CGL policies, can be construed restrictively, depending on its particular usage. Other exclusions beyond the intellectual property exclusion may also lead an insurer to deny coverage. For example, policies may exclude coverage for claims involving material first published or posted before the beginning of the policy period. Policies also typically exclude coverage for acts of the insured that are intended to, or could reasonably be expected to, cause injury. Thus, the conduct by the business must be inadvertent—which is arguably not the case with social media posting.

Media liability insurance is a type of professional liability or errors and omissions coverage that can protect retailers from copyright infringement lawsuits related to reproducing, distributing, performing or displaying a protected work without permission. Retailers who post media content such as web or social media content should consider adding media liability insurance to their risk management portfolio.

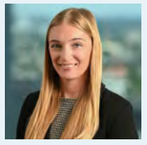
Cyber policies may also include coverage for copyright infringement claims under a media liability insuring agreement. If included, there is generally coverage for damages and claim expenses, including for legal costs and expenses resulting from the investigation and defense of the copyright infringement claim as well as damages that might result from a judgment or settlement. These damages, however, rarely include fines, penalties or future profits.

As a general matter, like all risks and types of insurance, retailers should understand their particular risk profile and all of the coverages and exclusions that compose their insurance portfolio to ensure there is adequate coverage and that all available insurance is pursued in the event of a claim.

Conclusion

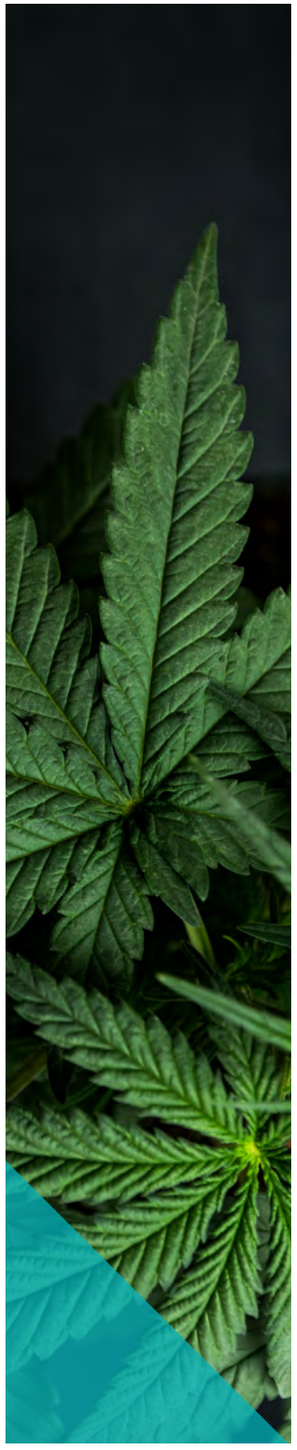
While retailers continue to embrace emerging marketing techniques through social media and the influencer culture, retailers should be diligent in their efforts to mitigate the risk presented by copyright infringement. Retailers should not assume that their current insurance program provides adequate coverage, as narrow definitions, exclusions or ambiguous policy language might present complexities or outright bars to coverage. Retailers should consult experienced insurance coverage professionals to ensure they have adequate coverage to protect against risks and potential exposure related to copyright infringement claims.





Michael Levine, Latosha Ellis and Veronica Adams
Michael is a partner and Latosha is counsel in the insurance coverage practice in the firm's Washington, DC office, and Veronica is an associate in the insurance coverage practice in the firm's Miami office.

Client relationships with more than half of the **20** largest retailers on the 2023 National Retail Federation's Top **100** Retailers List, representing retailers responsible for more than **$1.6 trillion** in US sales during 2022, including the two largest retailers in the country



Blazed and Confused: Balancing Workplace Safety with Expanded State Law Employment Protections for Cannabis Use

The rapid spread of marijuana legalization in states has slowed in recent years. But, recently passed laws in cannabis-friendly jurisdictions include expanded employment protections for medical and recreational cannabis users. The scope of the laws vary, but they generally make it more difficult for employers to discipline employees based on positive drug tests for THC, with several states requiring employers to show objective evidence of present impairment to support work-related penalties for marijuana use.

These laws have created significant issues for employers in how to reconcile state law compliance with occupational safety and health law compliance. OSHA law has not changed. The OSHA general duty clause and equivalent laws in state plan OSHA states still require employers to maintain a workplace free from recognized hazards that are causing or are likely to cause death or serious physical harm. Reasonable minds presumably should agree that a pallet jack operator who is high from THC could interfere with a safe workplace. Yet, some of these laws have no carve out regarding workers in safety-sensitive positions and steep requirements regarding reasonable suspicion drug testing. These conflicting rules leave employers in a hazy legal landscape that requires consideration of legal risks from varying sources and balancing operational priorities.

States Expand Employment Protections for Cannabis Users

Twenty-three states and Washington, DC, permit non-medical adult use of marijuana, and 38 states plus DC allow some type of medical use. When states first passed these laws, most legislatures remained silent on employment-related issues, which allowed employers to continue to include THC panels on their drug tests in spite of state-level legalization. But recently, states have passed additional regulations to provide more protections for marijuana users in the workplace.

As of January 1, 2024, more than 10 states restrict employers from taking adverse action against employees who test positive for marijuana, absent some other evidence of impairment. For example, New York prohibits employers from testing employees for THC at all, unless affirmatively required to do so by federal law. In Illinois, employers can test employees and applicants for THC, but cannot disqualify them from employment based on positive test results alone. And, most recently, California and Washington passed employment protections, effective January 1, 2024, that prohibit disqualification from employment for positive tests for "nonpsychoactive cannabis metabolites." Other states with restrictions include Arizona, Connecticut, Delaware, Iowa, Michigan, Montana, New Jersey, New Mexico, Oklahoma, Pennsylvania and Virginia, as well as Washington, DC. These laws support the idea that employees should not be tested for THC because the marijuana or cannabis product could have been consumed legally, off duty. Instead, employers must show some additional evidence of impairment or possession of marijuana *at work* to justify drug testing and/or discipline.

Workplace Safety Regulations Obligate Employers to Monitor Potential Impairment

State-level efforts to reduce employment barriers for marijuana users do not relieve employers of their obligation to maintain safe workplaces. Thus, employers have an obligation to take reasonable steps to prevent at-work impairment among employees whose job duties may pose a risk to themselves or their coworkers. Further, employers have business-related reasons in some states to maintain robust drug testing programs through workers' compensation premium incentives for employers with comprehensive drug testing programs and/or benefits exclusion for employees who test positive for drugs after being injured at work.

Several state laws regarding drug testing recognize potential conflicts with an employer's workplace safety obligations. For example, Connecticut and Washington's laws limiting the use of positive drug test results do not apply to employees in "safety-sensitive" positions. Other states, like New York and New Jersey, provide no such general exception for "safety-sensitive" roles. New York goes so far as to say employers cannot test employees for marijuana at all, or use the smell of marijuana or other "observable signs of use that do not indicate impairment," like bloodshot eyes, to support discipline. Instead, employers must rely on "objectively observable indications that the employee's performance of the duties of the position of their position are decreased or lessened," such as reckless operation of machinery. New Jersey allows drug testing and drug-free workplace policies

in certain circumstances, but does not allow employers to discipline based on positive tests for marijuana unless they also have "evidence-based documentation of physical signs or other evidence of impairment during an employee's prescribed work hours." Given the extent of some of the state law restrictions on drug testing and/or discipline, retailers should be sure they understand the details of the laws where they do business to determine what steps they lawfully may take to address potential impairment.

If states exempt safety-sensitive roles from their drug testing restrictions, then retailers need to analyze what roles might qualify for the exceptions. Some states define the term—for example, New Mexico defines a safety-sensitive position as "a position in which performance by a person under the influence of drugs or alcohol would constitute an immediate or direct threat of injury or death to that person or another."[1] Most states that define the term require some degree of foreseeable, serious injury based on the employee's job duties. For retail employers, it may be difficult to meet this standard at the store level. However, in distribution centers, employees operating powered industrial trucks or otherwise moving heavy material may well qualify as safety-sensitive employees. The unique facts of each job will determine whether an employee qualifies for a safety-related exception, so employers who wish to continue to use marijuana-related drug testing programs for disciplinary purposes in states with restrictions should analyze each position independently.

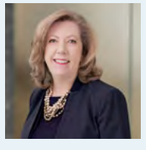
Employers Can Still Prohibit Impairment at Work—But Should Document Their Evidence

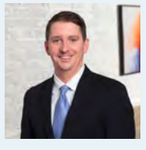
Retailers navigating the new patchwork of state laws regarding marijuana use should consider new ways to determine whether employees are impaired at work. Since many states prohibit reliance on positive tests alone, employers should look for evidence of present impairment. Generally speaking, employers can reduce their risk for taking adverse action against employees for marijuana use if they can support any discipline with objective evidence or symptoms that indicate impairment. For example, if an employer recognizes articulable symptoms of impairment like confusion, impaired speech, decreased responsiveness or poor job performance, then the employer should document that evidence to support potential adverse action. Ideally, employers would have at least two supervisors who observe and can attest to any evidence of impairment. Some states, including New Jersey, suggest training managers or supervisors on how to detect impairment to improve the reliability of any determinations that may lead to discipline.

Advice for Retailers—Study State Law Obligations, Then Balance Safety with Legal Compliance

The landscape of cannabis-related employment laws is cloudy. Retailers with existing drug testing or drug-free workplace policies should review the relevant laws in their states of operation to determine whether their programs may violate newly enacted protections for employees. But even if state laws purport to provide employment protections, retailers should understand that they have concurrent obligations to maintain a safe and healthful workplace. Thus, employers should consider whether state laws that protect employees from discipline may prejudice their ability to meet their workplace safety obligations. If so, then retailers should balance their dueling legal obligations—while a drug testing program designed to reduce risk of safety incidents at a distribution center might create some risk under state law, does it provide more value to the employer from a workplace safety perspective? Does the relevant state law provide employees with any real remedies that merit caution, or is it relatively toothless, supporting a more aggressive enforcement position from employers to support worker safety? The answers will likely vary by state, employer and even job position, but it's important that retailers understand the potential impact of these laws and make intentional choices about how to operate under them.

1 N.M. Stat. Ann. § 26-2B-3(Q)





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.

SEC Cybersecurity Disclosure Rules Take Effect

On July 26, 2023, the US Securities and Exchange Commission (SEC) adopted long-anticipated disclosure rules for public companies by a 3-2 party-line vote. The final rules apply to both US domestic public companies as well as any offshore company that qualifies as a "foreign private issuer" under SEC rules. The new rules took effect in December 2023, as detailed further below, and will likely require careful consideration by publicly traded retailers.

Background

Like the proposed version of the rules, the final rules require current reporting on Form 8-K (or Form 6-K for foreign private issuers) about the occurrence of material cybersecurity events, as well as an annual disclosure on Form 10-K (or Form 20-F for foreign private issuers) about corporate risk management, strategy and governance of cybersecurity. Unlike the proposed rules, the final rules do not contain a quarterly disclosure requirement under Form 10-Q (though periodic amendments of Form 8-K may be required), and the final rules contain no requirement to identify a board cybersecurity expert. The Form 8-K and Form 10-K reporting requirements were also modified from the proposed rules to take into account public comment on the proposal. The new rules explicitly exempt Canadian issuers who file Form 40-F and other SEC reports under the US-Canada multijurisdictional disclosure system, and such Canadian issuers should continue to make cybersecurity disclosures consistent with Canadian requirements.

Form 8-K and Form 6-K Reporting

Under the final rules, new Item 1.05 of Form 8-K requires disclosure of material cybersecurity incidents within four business days of the company's materiality determination. In response to commenters' concerns about the scope and timing of disclosure, the final rules make some modifications to the proposed version of the rules. Under final Item 1.05, if a public company experiences a "cybersecurity incident" that the company determines to be material, it must describe the material aspects of the nature, scope and timing of the incident, and the material impact or reasonably likely material impact on the company, including its financial condition and results of operations. For these purposes, a "cybersecurity incident" is defined under Item 106(a) of Regulation S-K, discussed further below. The untimely filing of an Item 1.05 Form 8-K will not result in the loss of Form S-3 eligibility for issuers conducting short-form securities offerings.

New Item 1.05 includes several explanatory instructions. First, a company's materiality determination regarding a cybersecurity incident must be made without unreasonable delay after discovery of the incident, which is intended to provide a limited amount of leeway to companies to avoid premature disclosure. Second, to the extent that the information called for in Item 1.05(a) is not determined or is unavailable at the time of the required filing, the company must include a statement to this effect in the filing and then must file an amendment to its Form 8-K filing under Item 1.05 containing such information within four business days after the company, without unreasonable delay, determines such information or within four business days after such information becomes available. This new requirement is intended to take the place of the quarterly Form 10-Q reporting requirement featured in the proposed version of the rules, and may necessitate multiple amendments over time to the original Form 8-K filing. Further, a company need not disclose specific or technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede its response or remediation of the incident.

The SEC's adopting release further explains that Item 1.05's inclusion of "financial condition and results of operations" is not exclusive, and companies should consider qualitative factors alongside quantitative factors in assessing the material impact of an incident. As an example, according to the SEC, "harm to a company's reputation, customer or vendor relationships, or competitiveness may be examples of a material impact on the company." Likewise,

the "possibility of litigation or regulatory investigations or actions, including regulatory actions by state and federal governmental authorities and non-US authorities, may constitute a reasonably likely material impact." The final rules include no exemption for providing disclosures regarding cybersecurity incidents on third-party systems, nor do the final rules include any safe harbor for information disclosed about third-party systems. Notably, the SEC did not adopt the proposed requirement for disclosure regarding the incident's remediation status, whether it is ongoing and whether data were compromised.

In response to concerns from commenters, the final rules include a narrow law enforcement exemption.

Specifically, disclosure on Form 8-K may be delayed for 30 days if the US Attorney General provides written notification to the SEC that national security or public safety would be impaired substantially by immediate disclosure. The rules also lay out procedures by which the Attorney General may extend the delay for additional periods of time. The Department of Justice and FBI recently published high-level guidelines to operationalize the delay provisions, but it remains to be seen how this exemption will work in practice, and whether affected companies will have sufficient time during the four-business-day window to avail themselves of the delay.

For foreign private issuers, Form 6-K is amended to add material "cybersecurity incident" to the list in General Instruction B of information required to be furnished on Form 6-K. In practice, this requirement will obligate foreign private issuers to report on material cybersecurity incidents they make or are required to disclose in a foreign jurisdiction to any stock exchange or to any securityholders.

Form 10-K and Form 20-F Reporting

The final rules create a new Item 106 to Regulation S-K concerning cybersecurity risk management, strategy and governance. Each of the components in Item 106 must be disclosed annually in a domestic public company's Form 10-K. The final rules also create an analogous annual reporting requirement for foreign private issuers filing Form 20-F. To avoid repetition, we summarize the Form 10-K requirements below, which apply mutatis mutandis to Form 20-F.

Defined Terms. Item 106(a) creates several new definitions, which for the most part are unchanged from the proposed versions:

"Cybersecurity incident" means an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity or availability of a registrant's information systems or any information residing therein.

"Cybersecurity threat" means any potential unauthorized occurrence on or conducted through a registrant's information systems that may result in adverse effects on the confidentiality, integrity or availability of a registrant's information systems or any information residing therein.

"Information systems" means electronic information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of the registrant's information to maintain or support the registrant's operations.

An element of the proposed rules that would have required companies to aggregate individually immaterial events for purposes of determining whether a cybersecurity incident has occurred has been eliminated in the final rules in favor of the final definition's use of the term "series of unrelated unauthorized occurrences." Still, the adopting release emphasizes that the term "cybersecurity incident" in the final rules is to be "construed broadly."

Risk Management. Item 106(b) of Regulation S-K requires a public company to describe the processes, if any, for assessing, identifying and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. In providing such disclosure, a registrant should address, as applicable, the following nonexclusive list of disclosure items:

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

Item 106(b) also requires a public company to disclose whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the company including its business strategy, results of operations or financial condition, and if so, how.

Governance. Item 106(c) requires a public company to describe the board of directors' oversight of risks from cybersecurity threats. If applicable, the company should identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the processes by which the board or such committee is informed about such risk. Item 106(c) further requires a public company to describe management's role in assessing and managing the company's material risks from cybersecurity threats. In providing such disclosure, a company should address, as applicable, the following nonexclusive list of disclosure items:

- Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise;
- The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation and remediation of cybersecurity incidents; and
- Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.

An instruction to Item 106(c) notes that in the case of a foreign private issuer with a two-tier board of directors, the term "board of directors" means the supervisory or nonmanagement board. In the case of a foreign private issuer meeting the requirements of 17 CFR 240.10A-3(c)(3), the term "board of directors" means the issuer's board of auditors (or similar body) or statutory auditors, as applicable.

A second instruction to Item 106(c) notes that expertise of management may include, for example, prior work experience in cybersecurity; any relevant degrees or certifications; and any knowledge, skills or other background in cybersecurity.

In a departure from the proposed rules, the SEC is not requiring public companies to identify a board cybersecurity expert.

Effective Dates

The Form 8-K and 6-K reporting requirement took effect for cyber incidents occurring on or after December 18, 2023, though smaller reporting companies will have a delay until June 15, 2024. The annual reporting requirement on Form 10-K or 20-F took effect for fiscal years ending on or after December 15, 2023. Thus, annual reports published in 2024 will generally require the inclusion of the new Item 106 disclosure.

Updates to Policies and Procedures

Implicit in the new rules is the notion that information technology and information security professionals within a covered public company must have a greater role in SEC disclosure decisions. The SEC has already brought several enforcement actions against public companies for inadequate disclosure or inadequate disclosure controls and procedures involving cyber incidents, largely stemming from a breakdown in communication between IT/IS personnel and financial reporting personnel, such that key details or impacts of a cyber incident were incorrectly reported to investors. As public retailers begin to prepare for the effectiveness of the new rules, they should also consider whether cyber incident response plans, disclosure committee charters, and other disclosure controls and procedures will require modification to ensure accurate reporting of material cyber events.

Scott Kimpel, Mayme Donohue and Hannah Flint

Scott is a partner in the capital markets practice, head of the ESG practice and head of the working group on blockchain and digital assets in the firm's Washington, DC office. Mayme is a partner in the capital markets practice and co-leads the AI, metaverse and emerging technologies practice in the firm's Richmond office. Hannah is an associate in the capital markets practice in the firm's Washington, DC office.

2023 Litigation Trends for PFAS-Containing Consumer Products and 2024 Preview

PFAS-related claims continued to be one of the fastest-growing areas of litigation in 2023. Although the focus of claims continues to be environmental, arising from alleged contamination of drinking water sources, new filings related to PFAS in consumer products continued to increase as well.

To date, PFAS consumer product claims have come primarily in the form of putative class actions, alleging 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 and breach of warranty. These claims have targeted a variety of consumer products, including food and beverages, food packaging, cosmetics, personal hygiene and care products, and clothing.

Despite increasing filings over the past several years, PFAS consumer product litigation is still in its infancy and relatively limited compared to the expansive number of pending PFAS environmental claims. Consumer product claims have been filed by only a handful of firms, primarily in federal courts in California,

New York and Illinois. Further, pending cases have made little substantive progress through the court system. Many of the earliest claims either resolved or were voluntarily dismissed. It was not until late 2022 and 2023 that decisions on motions to dismiss began to issue. Moreover, even in instances where dismissals have been granted, plaintiffs have generally been given leave to amend, leading to additional pleadings and motions practice. As such, it remains to be seen whether the majority of PFAS consumer product claims will survive to proceed to discovery and beyond.

For motions to dismiss that were decided in 2023, most court rulings came out in favor of defendants. Defendants' successes came under varying theories. At least three courts granted motions to dismiss for lack of standing. In these cases, defendants successfully argued that the limited product testing on which plaintiffs relied was insufficient to plausibly allege that the specific product plaintiffs purchased likewise contained PFAS. Thus, plaintiffs failed to plead an injury-in-fact necessary to establish standing. A similar ruling came in the Rule 12(b)(6) context, where a court held that plaintiff's reliance on "total organic fluorine" testing as a proxy for PFAS in the product was insufficient to plead that PFAS was actually present. In each of these cases, plaintiffs have filed amended complaints, and renewed motions to dismiss are now pending.

Motions to dismiss were also successful on other theories. At least one court ruled that marketing statements that a food product contained "only real ingredients" was not rendered deceptive by the presence of PFAS in the food's packaging because FDA statutes and regulations specifically exempt from ingredient lists any components that may migrate to food from packaging. Other courts ruled that a defendant's statements indicating that its products were safe or promoted health were not rendered deceptive by the presence of a particular type of PFAS in the product because plaintiff failed to allege that the particular PFAS was unsafe or that use of the product could impact health.

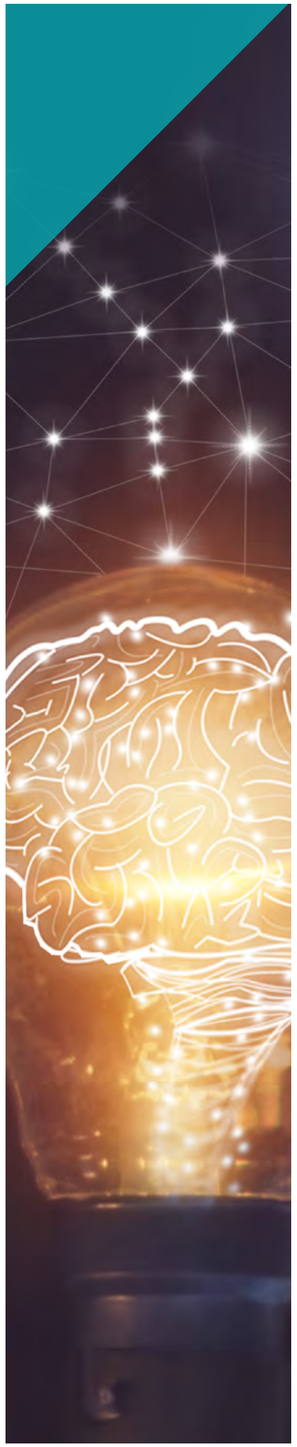
Plaintiffs' few successes at the motion to dismiss stage came (not surprisingly) in California. California courts considered similar challenges to those discussed above, but ruled the other way, concluding that plaintiffs' allegations were sufficient to proceed. Given the schedule for class certification briefing and fact and expert discovery, we do not expect to see summary judgment decisions or trial settings in these cases until at least 2025. Notably, another factor that may continue to drive PFAS claims in California is the state's "bans" on PFAS in certain consumer products. Unique from any other state, these laws not only preclude PFAS from being intentionally added to products but also prohibit total organic fluorine above certain levels. The latter aspect of these laws creates enhanced risk for defendants because impermissible levels of organic fluorine can be present in products merely because of the ubiquity of PFAS in the environment (e.g., in water and air) and not because of any intentional use of PFAS in the manufacturing process.

Another trend to watch in 2024 is the viability of medical monitoring as a remedy for consumer claims. Although these plaintiffs do not allege that they have suffered present health effects from exposure to PFAS in products, some seek damages for ongoing monitoring for future personal injuries or disease. If allowed to proceed, these claims drive up case values beyond those asserting mere economic harm. This risk could increase over the year ahead as a bellwether program for personal injury claims becomes a focus of the aqueous film-forming foam multidistrict litigation (AFFF MDL), which centralizes federal court claims arising from the use of PFAS in fire-fighting agents. The bellwether program will involve plaintiffs alleging that they developed certain diseases—kidney cancer, testicular cancer, hypothyroidism/thyroid disease and ulcerative colitis—as a result of exposure to PFAS from AFFF that entered drinking water sources. Although the alleged exposure scenarios at issue are very different from those that could arise in the consumer product context, outcomes in the MDL are likely to impact the trajectory of PFAS litigation more broadly.

Finally, in the year ahead, retailers should pay particular attention to any compliance obligations they may face under EPA's October 2023 final rule under the Toxic Substances Control Act that requires extensive reporting by entities that have manufactured or imported PFAS at any time since January 1, 2011. Retailers should further assess potential implications that compliance may have for future consumer litigation and strategize opportunities for risk mitigation in the meantime.

Alexandra Cunningham and Merideth Daly

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



EEOC Issues New AI Guidance in 2023

2023 saw the Equal Employment Opportunity Commission weigh in again on the use of artificial intelligence in the workplace. In May, the EEOC issued guidance regarding employers' use of AI in making employment decisions, such as hiring, promotions, demotions and terminations (the Guidance). The Guidance follows the EEOC's publication in 2022 regarding compliance with the Americans with Disabilities Act when using AI. According to the EEOC, the most recent Guidance was necessary because while employers may understand how to monitor for unintended discrimination when using traditional decision-making methods, they may not necessarily understand how to do so when using AI. The Guidance is particularly relevant to retailers given the volatility of their workforces and significant number of personnel decisions they have to make.

Disparate Impact Reminder

The Guidance reminds employers that Title VII of the Civil Rights Act of 1964 governs both intentional and unintentional discrimination when making employment decisions. Neutral tests and selection procedures that have a disproportionate adverse effect on applicant groups and employees protected under Title VII are called "disparate impact" discrimination.

The Uniform Guidelines Apply

The Guidance explains that the Uniform Guidelines on Employee Selection Procedures (Guidelines), which the EEOC adopted in 1978, remain applicable and provide direction for employers to assess any disparate impact their AI tools may have. Under the Guidelines, a "selection procedure" is any "measure, combination of measures, or procedure" employers use as a basis for an employment decision. Thus, according to the EEOC, the Guidelines would apply to "algorithmic decision-making tools when they are used to make or inform decisions about whether to hire, promote, terminate, or take similar actions toward applicants or current employees." Thus, retailers using AI in hiring, promotions, etc., should look to the Guidelines for Title VII compliance, according to the EEOC.

The Four-Fifths Rule

Employers may assess whether a selection procedure has a disparate impact on a protected group by determining whether the procedure selects individuals in that group "substantially" less than individuals in another group. As the Guidelines explain and the Guidance reconfirms, if an AI tool has an adverse impact on applicants or employees of a particular race, color, religion, sex or national origin, then the tool likely violates Title VII, unless the employer can show that the selection procedure is job related and consistent with business necessity.

To determine whether an employer's selection rate for one group is substantially different from the selection rate of another group, the Guidelines refer to what the EEOC calls the "four-fifths rule." Under this rule, one rate is substantially different from another if their ratio is less than four-fifths or 80 percent. The Guidance, however, explains that the four-fifths rule is simply a "rule of thumb" and "may be inappropriate under certain circumstances." For example, the rule may be inappropriate where AI makes a large number of selections and thus smaller differences may reflect an adverse impact on certain groups. The rule may also be inappropriate where an employer's actions discourage individuals in a protected group from applying. Thus, retail employers cannot necessarily rely on the "four-fifths" rule to ensure compliance with Title VII and may have to instead use more sophisticated statistical analyses to assess their AI tools.

Employer Responsibility for Vendors

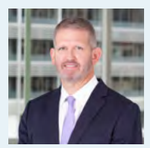
The Guidance confirms that employers may be held responsible for AI tools that create a disparate impact, "even if the tools are designed or administered by another entity, such as a software vendor." Further, the Guidance provides that employers "may be held responsible for the actions of their agents … if the employer has given them authority to act on the employer's behalf, " including in "situations where an employer relies on the results of a selection procedure that an agent administers on its behalf." Therefore, according to the EEOC at least, retailers cannot necessarily avoid liability for Title VII disparate impact discrimination by blaming the vendor's AI tool or a vendor's administration of a tool on the retailer's behalf.

Steps to Minimize Liability

Retailers should consider the following steps to minimize Title VII liability that may arise from using AI in employment decisions:

- stay informed about the developing legal framework for the use of AI in employment decision-making;
- understand the legal and statistical nuances of disparate impact discrimination;
- maintain human involvement with AI selection tools; and
- partner with an experienced employment attorney to conduct privileged audits of AI selection tools to assess disparate impact discrimination.

The last point is particularly important because, as the Guidance makes clear, the "EEOC encourages employers to conduct self-analyses on an ongoing basis" to determine whether a tool has a disparate impact on protected groups.



Kevin White and Michael Reed

Kevin is a partner, co-chair of the labor and employment team and co-chair of the retail and consumer products industry group in the firm's Washington, DC and Houston offices. Michael is an associate on the labor and employment team in the firm's Houston office.

Key Legal Issues in Data Breach Litigation

Robert Mueller, former director of the FBI, famously said that "there are only two types of companies: Those that have been hacked and those that will be." Recent data reflects that retail remains one of the most targeted industries for hackers, accounting for approximately 24 percent of all cyberattacks.[1] Because retailers often store large volumes of credit and debit card and banking information from customers, they can be a prime target for financially motivated cybercriminals.

As just a few examples, the Hudson's Bay Company—then-parent of Lord & Taylor and various Saks companies—settled a class action lawsuit last year for a $2 million cap on payments and up to $1.4 million in attorneys' fees. Plaintiffs in that case alleged that a criminal syndicate accessed cardholder information and sold it on the dark web. A leading retailer also recently faced a data breach affecting 4.6 million customers, resulting in a $1.6 million class action settlement finalized in 2021.

A review of recent case law involving retailers reveals emerging legal issues that can help companies prepare for and defend litigation arising from cybersecurity incidents. Indeed, at the motion to dismiss stage, almost all data breach cases include issues of (1) standing, (2) negligence-based claims and (3) contract-based claims.

1 Trustwave, 2020 Trustwave Global Security Report, https://www.trustwave.com/en-us//2020-trustwave-global-security-report/.

Standing

In federal court, the first inquiry usually is standing or injury-in-fact. Courts are split on what facts are necessary to establish standing in a data breach case, but certain patterns and trends can be identified.

There are several theories of harm that are commonly alleged in data breach cases: (1) actual identity theft or other misuse of personal data; (2) increased risk of future identity theft or other misuse; (3) loss of time and money responding to the breach or mitigating the harm; and (4) diminished value of the affected data. The second category is the subject of most litigation, as many data breach plaintiffs suffer no actual identity theft and therefore rely on a theory of increased risk of future harm. Whether Social Security numbers or other sensitive, immutable information is affected is paramount in this consideration.

In the breach affecting Lord & Taylor and Saks Fifth Avenue, the court found that plaintiff failed to state a substantial risk of future harm based on theft of debit card data because she canceled the card and froze the account. However, the court concluded that the time and money plaintiff spent obtaining a replacement debit card was sufficient to demonstrate injury-in-fact.[2] By contrast, in the Bonobos data breach, the court found that plaintiff did *not* state an injury-in-fact because "the stolen and posted information was all 'less sensitive data, such as basic publicly available information, or data that can be rendered useless to cybercriminals' " including customers' addresses, phone numbers, email addresses, IP addresses, encrypted passwords and partial credit card numbers.[3]

Negligence-Based Claims & Related Defenses

To state a claim for negligence, plaintiffs must show (1) a duty of care owed by the defendant, (2) breach of that duty, (3) proximate cause of the plaintiffs' injuries and (4) resulting damages. Often—but not always—resolving negligence claims requires a factual analysis after conducting discovery. Whether negligence claims

in the data breach context survive a motion to dismiss depends upon (1) whether a duty to safeguard data is recognized, (2) whether the economic loss doctrine applies and (3) the sensitivity of the data impacted.

The economic loss doctrine "bars a plaintiff from recovering for purely economic losses under a tort theory of negligence."[4] Courts in different jurisdictions apply the economic loss doctrine inconsistently, and appear to be trending toward rejecting it in the data breach context. Courts in New York have previously held the economic loss doctrine was not applicable,[5] whereas courts in other states—including Illinois, Kansas, Missouri,

2 *See Rudolph v. Hudson's Bay Co.*, No. 18-CV-8472 (PKC), 2019 WL 2023713, at *6 (S.D.N.Y. May 7, 2019).
3 *Cooper v. Bonobos, Inc.*, No. 21-CV-854 (JMF), 2022 WL 170622, at *4 (S.D.N.Y. Jan. 19, 2022).
4 *In re Capital One Consumer Data Security Breach Litig.*,488 F. Supp. 3d 374, 393 (E.D. Va. 2020).
5 *See, e.g., Rudolph*, 2019 WL 2023713, at *10 (denying the motion to dismiss based upon the economic loss doctrine).

Ohio and Pennsylvania—have dismissed negligence claims in data breach cases based upon this doctrine.[6]

Contract-Based Claims & Related Defenses

Plaintiffs that have a direct contractual relationship with the defendants will typically assert an express breach of contract claim, while plaintiffs that do not will often rely upon a theory of implied contract, third-party beneficiary contract or quasi-contractual theories such as unjust enrichment.

For example, in the Hudson's Bay case, while plaintiff did not have an express contract with Saks OFF 5TH, she alleged that by using her debit card, she entered into an implied contract under which defendants agreed to protect her card information. Applying California law, the court denied the motion to dismiss, holding that "an implied contract is formed where a person discloses sensitive information in order to receive a benefit, with the expectation that such information will be protected."[7] While implied contract claims against retailers tend to survive motions to dismiss in the data breach context, the Eleventh Circuit recently affirmed dismissal of such a claim—concluding that plaintiff failed to adequately state a "meeting of the minds" regarding the key contractual provisions.[8]

Conclusion

This is only a brief summary of some of the most common legal issues to emerge early in data breach litigation. The ultimate resolution of these claims depends upon the nature of the data affected, specific circumstances of the named plaintiff(s), abilities of counsel, and the jurisdiction and court in which the case is filed. It is thus important to retain highly experienced and skilled counsel in the area of data breach litigation.

Perie Reiko Koyama and Susan Shin

Reiko is counsel in the antitrust and consumer protection practice in the firm's Washington, DC office, and Susan is a partner in the corporate and securities litigation practice in the firm's New York office.

6 *See, e.g., Perdue v. Hy-Vee, Inc.*, 455 F. Supp. 3d 749, 761–62 (C.D. Ill. 2020); *Newman v. Total Quality Logistics, LLC*, No. 1:20cv173, 2021 WL 1192669, at *7 (S.D. Ohio Mar. 30, 2021); *Longenecker-Wells v. Benecard Servs., Inc.*, 1:15-CV-00422, 2015 WL 5576753, at *5 (M.D. Pa. Sept. 22, 2015).

7 *Rudolph*, 2019 WL 2023713, at *11.

8 *See Ramirez v. Paradies Shops*, LLC, 69 F.4th 1213, 1221 (11th Cir. 2023).

Washington, Nevada and Connecticut Enact Health Privacy Laws

Washington, Nevada and Connecticut recently adopted health privacy legislation adding new state protections for consumer health data. Unlike the federal Health Insurance Portability and Accountability Act (HIPAA), which applies only to certain health care entities and their business associates, these new state health privacy laws apply to a broad range of entities, including in the retail sector. We anticipate a continued regulatory and enforcement focus on sensitive personal data, including health data, at both the state and federal levels in 2024, and these laws are poised to impact a number of companies that might otherwise have relatively low exposure to health privacy regulation.

Applicability

In April 2023, Washington enacted the My Health My Data Act (WMHMDA), the first state comprehensive consumer health data privacy law in the United States. The WMHMDA applies to "regulated entities" and "small businesses" that (1) conduct business in Washington or offer products or services targeted at consumers in Washington and (2) determine the purpose and means of collecting, processing, sharing or selling of consumer health data. The WMHMDA's definition of "consumer health data" is extremely broad and the nonexclusive list of examples includes personal information that identifies a consumer's past, present or future "physical

or mental health status." Physical or mental health status includes individual health conditions, treatment, diseases or diagnoses and use or purchase of prescribed medications (but does not explicitly exclude non-prescription medications). It also includes precise location information "that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies." In addition, certain requirements, such as the WMHMDA's geofencing prohibition, discussed below, apply to any "person" (i.e., not only regulated entities).

In June 2023, shortly following the passage of the WMHMDA, Connecticut and Nevada enacted their own health privacy laws. Nevada's health privacy law, S.B. 370, is similar to the WMHMDA in terms of applicability and structure. However, the Nevada law has a slightly more narrow definition of "consumer health data" that applies only where the regulated entity uses the information to identify the consumer's health status. Nevada's definition is otherwise much like Washington's in that it includes a long list of examples.

Connecticut's health privacy law, S.B. 3, enacted as an amendment to the Connecticut Data Privacy Act, follows Nevada's approach in defining "consumer health data" more narrowly to mean any personal data that a controller "uses to identify" a consumer's physical or mental health condition or diagnosis, and includes, but is not limited to, gender-affirming health data and reproductive or sexual health data. Unlike Washington and Nevada, Connecticut's definition does not otherwise include a long list of examples. The law applies to entities that process the consumer health data of Connecticut residents.

General Requirements

Both the Washington and Nevada laws impose a number of obligations on regulated entities, including to develop and maintain a consumer health data privacy policy; comply with certain consumer rights requests; maintain administrative, technical and physical data security practices; and enter into contracts that meet specific requirements with processors that process consumer health data.

All three new state laws require entities to obtain consent prior to certain disclosures (e.g., selling) of consumer health data and restrict access to consumer health data by employees, processors and other entities. In addition, in many cases, separate consent is required for the collection of consumer health data.

Geofencing Ban

In Washington and Nevada, any person (i.e., not only regulated entities) is prohibited from establishing a geofence around an entity that provides in-person "health care services," where the geofence is used to (1) identify or track consumers seeking health care services; (2) collect consumer health data from consumers; or (3) send notifications, messages or advertisements to consumers related to their consumer health data or health care services. Notably, "health care services" are broadly defined to include any service "provided to a person to assess, measure, improve, or learn about" a person's mental or physical health, and specifically includes use or purchase of medication (i.e., not just prescription medication). Retail companies may be subject to this prohibition, if, for example, they sell over-the-counter medications or other health-related products.

Connecticut's geofencing provision is a bit more narrow, prohibiting the use of a geofence around "any mental health facility or reproductive or sexual health facility for the purpose of identifying, tracking, collecting data from or sending any notification to a consumer" regarding their health data.

Enforcement

All three laws provide for government enforcement, but the WMHMDA also provides for a private right of action. Most of the WMHMDA's substantive provisions will not apply until March 31, 2024.

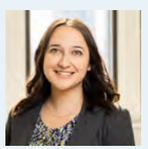
Notably, the law's geofencing prohibition is already in force. Certain provisions of Connecticut's health privacy law are in force, but others, such as those relating to the protection of minors, will not apply until October 1, 2024. Nevada's law will take effect on March 31, 2024.

Next Steps in 2024

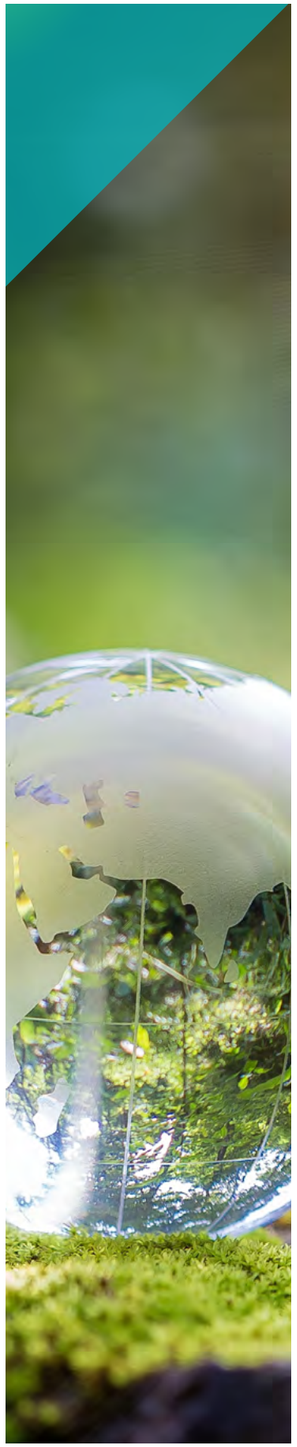
Retail companies should take a conservative approach when interpreting the scope of these new laws. This will help to mitigate risk of liability, particularly as we anticipate regulatory and enforcement efforts to focus on this area and in light of the private right of action under Washington's law. Companies should assess the applicability of these laws to their businesses to determine next steps to take for compliance, which may include development of privacy notices, consent procedures, rights request response processes and processor contracts, among others.

Retail team is recognized by *Chambers USA* in the Nationwide Retail category, while individual lawyers are recognized in their respective practice areas, globally, nationally and regionally



Michael La Marca, Marshall Mattera, Jennie Cunningham and Liliana Fiorenti
Michael is a partner, Marshall and Jennie are associates, and Liliana is a law clerk in the global privacy and cybersecurity practice in the firm's New York office.



Legal Considerations for Corporate Circular Economy Strategies

Over the past several years, circular economy goals have become nearly ubiquitous in corporate sustainability strategies. This trend is driven by a number of factors, including consumer interest in sustainable products, opportunities for generating circular revenue (i.e., generating revenue at multiple points in a product's life cycle, such as through product collection and refurbishing) and the presence of circular economy metrics in commonly used voluntary sustainability standards, such as those issued by the Global Reporting Initiative (GRI) and Sustainability Accounting Standards Board (SASB). Recent legal and policy developments in multiple markets may counsel in favor of reassessing existing corporate strategies related to circular economy. To maximize the value of existing efforts, companies should consider three categories of legal developments when setting or reassessing circular economy goals: government incentives, regulations and reporting and disclosure requirements.

The US Environmental Protection Agency describes "circular economy" as "a change to the model in which resources are mined, made into products, and then become waste. A circular economy reduces material use, redesigns materials, products and services to be less resource intensive, and recaptures 'waste' as a resource to manufacture new materials and products." Environmental benefits include waste and pollution reduction, as well as reduced greenhouse gas emissions. In addition, circular economy efforts can help promote supply chain security by reducing reliance on imports. In recognition of these benefits, governments in many jurisdictions have started to develop new legal frameworks to promote circular economy efforts. Notably:

- In 2020, the European Union (EU) adopted a Circular Economy Action Plan. The EU continues to develop new regulatory and policy actions in support of the plan.
- In 2022, the United States passed the Inflation Reduction Act, the CHIPS and Science Act, and the Bipartisan Infrastructure Law, all of which contain provisions targeted at promoting circularity and recycling.
- A number of US states have adopted or are considering laws that require producers to increase use of post-consumer content and/or take responsibility for end-of-life products or packaging.

Incentives

Companies that sell certain types of products—especially products related to renewable energy infrastructure, such as batteries or solar panels—have increasing access to economic incentives targeted at creating a domestic circular supply chain. For example, in the Inflation Reduction Act of 2022, Congress amended the definition of "new clean vehicle" to allow for electric vehicle (EV) battery materials recycled in North America, regardless of their origin, to qualify for the US clean vehicle tax credit. This incentivizes companies to establish domestic recycling facilities by creating consumer demand for domestically recycled EV batteries. Understanding available economic incentives and the criteria for obtaining them is now a critical step in making decisions about product design and sourcing.

Regulations

New regulations targeted at achieving circular economy goals address both product design and end-of-life management.

In the packaging context, several jurisdictions have begun to impose legal requirements for source reduction or recycled content that will help shape these efforts going forward. Notably, Washington, California, New Jersey, Maine and Connecticut have all passed laws mandating certain levels of post-consumer content in packaging products, and administrative rulemaking to further define requirements is underway in all these states.

Increasingly, producers will also need to take responsibility for products at the end of their life after they have been in the hands of consumers. Several states have passed or proposed extended producer responsibility (EPR) legislation for single-use packaging, often in combination with recycled content requirements. These programs have broad applicability and may affect companies that sell products in many different industries.

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

As in the incentive space, US EPR programs have also targeted renewable energy technologies, including solar panels, wind turbines and batteries. Washington is leading the nation with the Photovoltaic Module Stewardship and Takeback Program, an EPR program for solar panels, and also recently passed legislation to study the feasibility of wind turbine blade reuse and recycling. Washington, California and the District of Columbia have also established EPR programs for small primary or portable batteries (i.e., common household batteries), and California is considering legislation that would create an EPR program for end-of-life EV batteries.

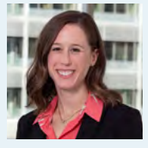
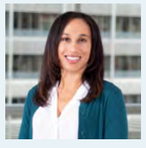
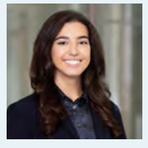
Reporting and Disclosure Requirements

A third type of legal development that companies will increasingly need to consider when developing circular economy-related strategies is reporting and disclosure requirements. These laws are aimed at standardizing how companies report on their sustainability efforts. Depending on who a company's stakeholders are and how they are expected to react to new reporting, companies may need to consider whether any operational changes are needed in areas where disclosures are required.

As noted above, many companies have already been reporting on circular economy efforts under voluntary reporting standards. Now, the shift to mandatory reporting has begun. In July 2023, the European Commission, acting in accordance with the EU's Corporate Sustainability Reporting Directive, adopted a Sustainability Reporting Standard on Resource Use and Circular Economy known as ESRS E5. Companies subject to ESRS E5 will need to report on company policies, goals and actions related to circular economy efforts, such as use of recycled resources, transition away from virgin materials and sustainable sourcing. So far, there has not been push toward mandatory reporting for circular economy efforts in the United States. Companies operating in the United States, however, need to be careful about how they publicize their efforts. The Federal Trade Commission is currently revising its Guides for the Use of Environmental Marketing Claims (Green Guides) and, during the rulemaking process, sought public comment on updating its guidance regarding "recycled content" claims.

Conclusion

Given these changes in the legal landscape, collaboration between corporate sustainability teams and legal counsel will be increasingly important when setting, and monitoring progress toward reaching, circular economy goals.

Rachel Saltzman, Erin Grisby and Abigail Contreras

Rachel is a partner and Erin is an associate on the environmental team in the firm's Washington, DC office, and Abigail is an associate on the environmental team in the firm's San Francisco office.

Key Contacts

Robert Quackenboss
Partner
+1 202 955 1950 (Washington, DC)
+1 212 309 1336 (New York)
rquackenboss@HuntonAK.com

Bob is the editor of the 2023 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
+1 202 419 2101 (Washington, DC)
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.

Kevin White
Partner
+1 202 955 1886 (Washington, DC)
+1 713 229 5708 (Houston)
kwhite@HuntonAK.com

Kevin is co-chair of the firm's labor and employment team and co-chair of the firm's retail and consumer products industry group. He has a national practice that focuses on complex employment litigation, employment advice and counseling, and labor relations.

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 for more information on our industries and practices.

23849-02.24