HUNTON
ANDREWS KURTH

2018

RETAIL INDUSTRY

YEAR IN REVIEW

Published in January 2019




TABLE OF CONTENTS




DEAR CLIENTS AND FRIENDS,

It has been a very exciting year for our law firm and our retail clients. In April 2018, two preeminent firms, Hunton & Williams and Andrews Kurth Kenyon, merged to form Hunton Andrews Kurth LLP. With 1,000 lawyers in the United States, Asia, Europe and the Middle East, the combined firm serves retail and consumer products clients across a broad range of complex transactional, litigation and regulatory matters. The combination has enhanced the quality, depth and breadth of our substantive legal practice areas, as well as our ability to provide innovative legal solutions to our retail clients.

Our retail team, comprised of more than 200 lawyers across practices, represents national and global supermarket chains, restaurants, home improvement warehouses, media and entertainment companies, toys and baby product manufacturers and distributors, electronics manufacturers and distributors, high-end apparel retailers, consumer services retailers and more on all matters of law. We are pleased to be recognized by *Chambers USA* as one of the top retail groups in the country, which reflects our efforts and accomplishments on behalf of our retail clients and our deep understanding of issues facing the retail industry.

Our 2018 *Retail Industry Year in Review* provides a broad overview of recent developments that retailers have faced, as well as a look ahead at what they can expect in 2019. The emergence and increasing use of new technologies such as blockchain, biometrics and cashless stores, as well as several developments impacting employers and consumer privacy, made 2018 a unique, challenging and innovative time for the retail industry. Hunton Andrews Kurth's retail team is at the forefront of these issues and achieved several successes on behalf of our retail clients in the past year. Recent highlights include:

- We represent one of the world's largest retail food groups in its federal antitrust lawsuit against several of the nation's largest chicken producers, alleging the companies conspired for nearly a decade to fix chicken prices by reducing the supply and manipulating a key industry benchmark price index.
- We successfully defended several prominent retailers against false advertising claims.
- We advised a retail business group on a data security issue involving the payment card data of customers at three of its portfolio department stores. We handled the companies' incident response activities, including directing a leading forensic security team, conducting the legal analysis, preparing the relevant notifications and communication materials and responding to regulatory inquiries following the announcement of the incident.
- We successfully represented a leading consumer products manufacturer in an ITC patent litigation matter.

I hope that our 2018 *Retail Industry Year in Review* gives you a fresh view of current business realities and a forward-looking perspective on emerging issues for the retail industry.

Wally Martinez
Managing Partner

INSURANCE COVERAGE DEVELOPMENTS IN 2018



Syed Ahmad, Sergio Oehninger and Daniel Hentschel

Syed is a partner and Sergio is counsel in the insurance coverage practice in the firm's Washington office. Daniel is an associate in the insurance coverage practice in the firm's Miami office.

Cyber Coverage for Social Engineering Schemes Remains at Odds

Social engineering continued to be a major concern in 2018 as businesses continued to fall prey to such schemes and other cyber risks. 2018 also saw a trend in favor of coverage for these schemes, which is promising for retailers and other businesses. However, the varied results continue and should caution policyholders to obtain social engineering/impersonation cyber fraud coverage by endorsement that is as specific as possible.

- **Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am.**, 895 F.3d 455 (6th Cir. 2018). The Sixth Circuit reversed a district court's decision finding coverage under a crime policy for a manufacturer's $800,000 loss, reasoning that the fraudulent email that prompted wire transfers to fraudsters was an immediate and proximate cause of the loss.
- **Medidata Sols. Inc. v. Fed. Ins. Co.**, 268 F.Supp.3d 471 (2d Cir. 2018). The Second Circuit affirmed a district court's ruling and found coverage under the computer fraud provision of the insured's crime policy for a cloud-based service provider's loss of $4.8 million resulting from an employee's being deceived into transferring the money as a result of an email disguised to look like it was from the company's president.
- **Aqua Star (USA) Corp. v. Travelers Cas. & Surety Co. of Am.**, No. 16-35614 (9th Cir. Apr. 17, 2018). The Ninth Circuit affirmed a district court's decision finding no coverage for a $700,000 loss resulting from hackers who, while posing as employees, directed other employees to change account information for a customer. The court found that an exclusion providing that the policy "will not apply to loss resulting directly or indirectly from the input of Electronic data by a natural person having the authority to enter the Insured's Computer System" applied and barred coverage.

Contrasting Results Introduce New Challenges for Policyholders Seeking Coverage for Credit Card Company Assessments and Penalties Resulting from Cyber Exposure

Businesses are increasingly purchasing insurance policies to address their cyber and data security exposures. Recently, courts have weighed in on coverage afforded to policyholders for credit card company assessments and penalties resulting from data exposure caused by third-party hackers. Many of the judicial decisions addressing insurance for cyber exposures have done so under traditional insurance policies, as opposed to under newer cyber insurance policies, resulting in negative results for policyholders. However, recent decisions demonstrate that policyholders should engage their insurers to ensure that their policies, whether traditional or not, are specifically designed to cover cybersecurity and data breach events. And, faced with a denial, policyholders should not assume that an insurer's efforts to deny coverage will necessarily prevail in all cases, as shown by recent decisions.

- **Spec's Family Partners, Ltd. v. Hanover Ins. Co.**, No. 17-20263 (5th Cir. June 25, 2018). The Fifth Circuit found that Hanover Insurance Company had a duty to defend Spec in an action arising out of two data breaches of Spec's credit card payment system. The court held that the district court improperly found that an exclusion for contract-based claims barred coverage, finding that part of the alleged conduct did not fall within the exclusion for contract-based claims.

- **St. Paul Fire & Marine Insurance Co. v. Rosen Millennium Inc.**, 6:17-cv-540 (M.D. Fla. Sept. 28, 2018). A federal district court in Florida ruled that St. Paul Fire & Marine Insurance Co.'s commercial general liability policy did not cover fines and penalties assessed against its insured, Rosen Hotels, after hackers installed malware into the hotel's credit card payment network. The court reasoned that the policy required that the credit card information be "made known" by the insured's activities and not a third party's activities. Thus, because the credit card information was made known as a result of the hackers' activities, the court found there was no coverage.

Recall Insurance Continues to be Source of Coverage Disputes

The risk of product recalls has continued to increase in recent years due to tightened regulatory standards and the implementation of new safety rules. 2018 experienced a surge in coverage disputes involving the interpretation of recall insurance policies' terms. Varying court interpretations illustrate the need for policyholders to scrutinize recall insurance policies. Below we highlight some key cases.

- **Blessings, Inc. d/b/a Blessings Seafood v. Houston Casualty Co.**, No. 1:18-cv-00262-LTS (S.D.N.Y. filed Jan. 11, 2018). A seafood distributor, Blessings, sued its insurer seeking to recover losses associated with a product contamination claim involving Blessings' raw shrimp product. Blessings sought coverage under its contamination policy with Houston Casualty, which provided coverage for, among other things, the value of contaminated products up to $3 million per insured event. Houston Casualty issued partial payment for Blessings' direct losses associated with the value of the contaminated shrimp, but refused to pay the balance of the claim. On March 1, 2018, the court was notified that the parties had reached a settlement, pending execution of a final written agreement.
- **Hanover Ins. Group, Inc. v. Raw Seafoods, Inc.**, 91 Mass. App. Ct. 401 (2107). The Appeals Court of Massachusetts in Boston found that the trial judge erred when granting summary judgment in favor of the insurer relating to a coverage dispute regarding more than 57,000 pounds of spoiled scallops. RSI, a seafood processing company, was sued by its customer, Atlantic Capes Fisheries Inc., after receiving a batch of spoiled scallops for processing. RSI's insurer, Hanover, agreed to defend RSI in the action under a reservation of rights. Hanover also filed suit seeking a ruling that it owed no coverage because the damage to the products was not caused by an "occurrence" distinct from RSI's performance of its work. The trial court granted summary judgment in Hanover's favor, but the appellate court reversed, finding that the damaged scallops were caused by an "unexpected happening," and thus an "accident," rather than a foreseeable consequence of RSI's normal business operations.
- **Starr Surplus Lines Insurance Co. v. Mountaire Farms, Inc.**, No. 2:18-cv-67-JDL (D. Me. Aug. 02, 2018). A federal district court in Maine ruled against an insurer's effort to be reimbursed for $10 million it paid a policyholder in connection with salmonella-contaminated raw chicken. Starr Indemnity & Liability Co. Inc. brought an action against a chicken supplier, Mountaire Farms, asserting that Mountaire delivered contaminated chicken products to Starr's insured, AdvancePierre Foods, which resulted in a recall of more than 1,700,000 pounds of chicken products. Starr had paid the policy limits of $10 million for AdvancePierre's recall insurance claim. Mountaire moved to dismiss Starr's lawsuit, arguing, among other things, that Starr's claims failed because salmonella is an "inherent and recognized characteristic" of raw chicken and, therefore, could not be considered "defective," "unfit for its particular purpose" or "unreasonably dangerous," which are required elements of Starr's claims. Mountaire further argued that Starr's strict liability claim is barred by the economic loss doctrine. The court agreed with both arguments and dismissed the lawsuit.

#METOO BRINGS NEW CHALLENGES TO RETAILERS

Kevin White and Madalyn Doucet

Kevin is a partner and co-head of the labor and employment team and Madalyn is an associate on the labor and employment team in Hunton Andrews Kurth's Washington office.

In October 2017, *The New York Times* and *The New Yorker* published accusations of sexual harassment and abuse against Hollywood producer Harvey Weinstein. That watershed moment sparked what's been called a "national reckoning" over sexual harassment, driven heavily by the #MeToo movement going viral. In the year that has passed since then, this movement has only grown larger and louder. Other viral campaigns like #TimesUp and #BelieveWomen have pervaded the public consciousness. No industry has escaped untouched, including retail.

Business leaders and HR professionals are anecdotally reporting an increase in internal complaints about sexual harassment in the workplace. On the anniversary of the Weinstein scandal, the US Equal Opportunity Commission released early numbers confirming that trend: while overall discrimination complaints were down, the percentage of charges alleging sexual harassment increased by 12 percent, representing the first increase in the last 10 years. The EEOC itself brought 41 lawsuits in FY2018 alleging sexual harassment—a 50 percent increase over the previous year. Several of these were against retailers, big and small.

For retail companies that are publicly traded, there is another litigation risk bubbling from the sexual harassment reckoning: investor lawsuits brought by shareholders to hold companies accountable for sexual misconduct in the executive ranks. Two such high-profile suits have been brought against Wynn Resorts and CBS after their respective CEOs were accused of sexual misconduct and stock prices plummeted.

In addition to these increased risks, retailers must also ensure compliance with the ever-changing landscape of legislative responses to #MeToo.

Sexual Harassment Settlements

A number of laws enacted in the wake of #MeToo will affect how retailers may settle claims of sexual harassment.

At the federal level, the so-called "Weinstein Tax" was passed as a last-minute addition to the Tax Cuts & Jobs Act of 2017. A new section was added to the Internal Revenue Code to make settlements of sexual harassment and abuse claims subject to confidentiality agreements nondeductible. Due to ambiguous language in the provision and a dearth of guidance from the IRS, exactly how the IRS will treat these settlements is yet to be determined. Retailers should consider whether to allocate settlement payouts among claims, assign the settlement of sexual harassment or abuse claims nonmonetary consideration, or exclude altogether sexual harassment or abuse claims from nondisclosure provisions.

New state laws also prohibit or restrict the use of confidentiality or non-disclosure clauses in settlements of sexual harassment claims. Six states have passed such laws—Arizona, California, New York, Tennessee, Vermont and Washington—and at least three other states (Massachusetts, New Jersey and Pennsylvania) and the District of Columbia have proposed similar legislation. Retailers in Maryland should also be aware of a unique law that passed recently, requiring companies to report information about sexual harassment settlements for use in a survey.

Arbitration of Sexual Harassment Claims

Many of the laws proposed in response to #MeToo prohibit mandatory arbitration of sexual harassment claims. Maryland, New York, Vermont and Washington have all enacted such laws. Similar arbitration bans are pending in Congress and at least three other states (Massachusetts, New Jersey and South Carolina).

Anti-Sexual Harassment Policies and Training

Before #MeToo, it was rare for a state or local law to require anti-sexual harassment training or written policies by private employers. But after #MeToo, a wave of such laws has passed. California, one of the only states to have these requirements for private employers before #MeToo, expanded the reach of its training and policy requirement to even smaller employers. For retailers operating in New York and New York City, both have passed sweeping anti-sexual harassment laws that are not coterminous and require various combinations of training, policies and postings. In addition, Massachusetts, Pennsylvania, Vermont and Washington have also all proposed or passed laws that will require retailers to maintain written policies or conduct anti-sexual harassment training.

The #MeToo movement is a wake-up call to all retailers. Companies should take this opportunity to evaluate their policies regarding sexual harassment, train their employees and management on how to respond, consult with counsel regarding settlement and arbitration of these claims and promote a workplace culture that respects all employees.

ANTITRUST ENFORCEMENT STILL UNPREDICTABLE UNDER TRUMP

Kristina Van Horn and Andrew Eklund

Kristina is counsel and Andrew is an associate in the competition and consumer protection practice in Hunton Andrews Kurth's Washington office.

After a slow start in getting Senate-confirmed appointees in place, both the Department of Justice's Antitrust Division and Federal Trade Commission finally got their full complement of senior leadership in place in September 2018. Chairman Joe Simons and Commissioner Christine Wilson returned to the FTC as commissioners after years of private practice, and other major Commission roles have been filled by FTC alumni. Similarly, the Antitrust Division leadership has a number of attorneys with prior government experience.

This seasoned leadership, however, has not made antitrust enforcement more predictable. This uncertainty is even more pronounced in "vertical" deals involving companies that are at different levels of the supply chain. Both FTC and DOJ spoke out early in the Trump administration against behavioral remedies which have been used in the past to mitigate risk of harm to competition from vertical deals.[1]

Absent imposing behavioral remedies like those in Comcast/NBCU, the Division, for example challenged the proposed vertical transaction involving AT&T and Time Warner. This uncertainty is also present in horizontal deals involving direct competitors: some deals are getting inquiries where none were expected and some are being cleared when we expected inquiries.

On a more positive note, both the FTC and Antitrust Division have focused on process improvements. In response to increasing time, expense and burden of government antitrust investigations, both agencies have announced initiatives to speed up the review process for proposed mergers.[2]

[1] Asst. Att'y Gen. Makan Delrahim, Keynote Address at American Bar Association's Antitrust Fall Forum (Nov. 16, 2017) (noting a plan to "return to the preferred focus on structural relief to remedy mergers"; Bureau of Competition Acting Director D. Bruce Hoffman, "Vertical Merger Enforcement at the FTC," (Jan. 10, 2018) ("First and foremost, it's important to remember that the FTC prefers structural remedies to structural problems, even with vertical mergers.").

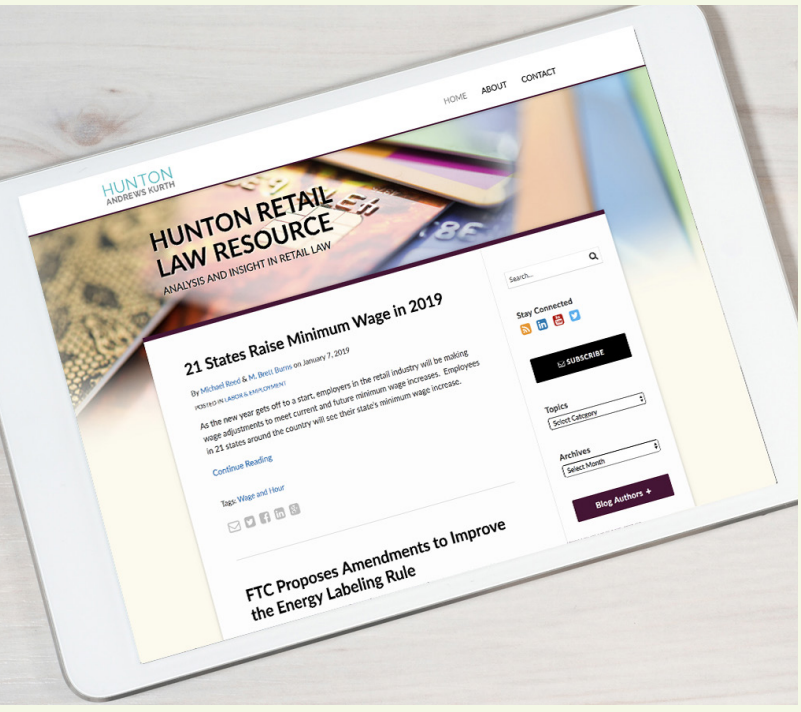
[2] Asst. Att'y Gen. Makan Delrahim, "It Takes Two: Modernizing the Merger Review Process," Remarks Before the 2018 Global Antitrust Enforcement Symposium (Sept. 25, 2018); Bureau of Competition Director D. Bruce Hoffman, "Timing is everything: The Model Timing Agreement" (Aug. 7, 2018), *available at* https://www.ftc.gov/news-events/blogs/competition-matters/2018/08/timing-everything-model-timing-agreement.

BTI Most Recommended Law Firms, August 2018

Several major retail mergers made headlines in 2018 and provide lessons for merging parties in 2019.

- **J.M. Smucker's attempted acquisition of the Wesson cooking oil brand from Conagra** was abandoned by the parties after the FTC challenged the merger. The FTC alleged that the combined Smucker's, which already owns the Crisco brand, would control at least 70 percent of the market for branded canola and vegetable oils sold to grocery stores and other retailers. The FTC also alleged that Smucker's own documents showed that eliminating price competition between Wesson and Crisco was a central part of the rationale for the deal. Interestingly, the FTC did not include private label cooking oils in its relevant market definition despite the fact that private label products account for a majority of cooking oil sales to retail consumers. Three days after the FTC filed for a preliminary injunction, the parties abandoned the deal.
- **AT&T's acquisition of Time Warner** was challenged by the Department of Justice in late 2017. After a full trial on the merits of the proposed acquisition, federal district court Judge Richard Leon approved the deal in June 2018 and the parties closed on the transaction soon thereafter. After initially saying that it would not challenge Judge Leon's decision, the DOJ appealed to the DC Circuit. AT&T has agreed to hold the Turner Networks (such as CNN, TNT, TBS and HLN) separate from the rest of its operations until February 28, 2019, and the parties have sought expedited treatment for the appeals process.

With two major mergers now facing additional scrutiny, 2019 is sure to bring additional drama to the antitrust landscape in the retail sector.



CLIENT RESOURCE: HUNTON RETAIL BLOG

www.huntonretailindustryblog.com

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

Subscribe now to Hunton Retail Law Resource for the latest legal updates, developments and business trends that affect your retail business.

FORMALDEHYDE CONTROVERSY RAISES CONCERNS FOR RETAILERS OVER EPA'S FUTURE REVIEW AND REGULATION OF CHEMICALS AND ASSOCIATED LITIGATION RISK

Alexandra Cunningham and Elizabeth Reese

Ali is a partner and co-head of the product liability and mass tort litigation practice and Elizabeth is an associate in the product liability and mass tort litigation practice in Hunton Andrews Kurth's Richmond office.

Companies in the retail industry may soon be grappling with new regulations and increased litigation risk involving formaldehyde, a common chemical found in consumer products like wood glue, foam insulation, paints, cosmetics and fragrances. In 2018, amid controversy over the chemical industry's alleged pressure on the Environmental Protection Agency (EPA) to withhold an updated human health risk assessment, which will reportedly link exposure to formaldehyde to leukemia and other cancers, consumer groups successfully compelled EPA to begin early enforcement of its new rule governing formaldehyde emissions from composite wood products. The tug-of-war between consumer groups and industry groups on formaldehyde over the last year has potential consequences for companies impacted not only by the formaldehyde regulations, but who may also be impacted by regulations on the horizon as EPA moves forward with its new risk evaluations on 10 "high priority" and widely used chemicals.

EPA's Integrated Risk Information System Program (IRIS) first classified formaldehyde as a "probable human carcinogen" in 1991, linking exposure to the chemical as potentially causing nasal cancer. In 2010, the agency released a new draft risk assessment, proposing to revise formaldehyde's classification to "carcinogenic to humans" and linking formaldehyde exposure to leukemia for the first time. The scientific data and methodology underlying the revised risk assessment were met with sharp criticism. In response, EPA requested that the National Research Council (NRC), a committee of the National Academies of Sciences (NAS), perform a peer review of the draft risk assessment. The NRC reported in 2011 that EPA's conclusions regarding leukemia and related hematopoietic cancers suffered from serious "data gaps" and were not supported by any clear scientific framework. The NRC also issued specific recommendations for the revision of not only the draft risk assessment itself, but also the overall review process for future assessments. Congress then directed EPA to implement the NRC's recommendations, and EPA began the process of re-reviewing its risk assessment to take into account the NRC's recommendations.

IRIS completed the update to its formaldehyde risk assessment in late 2017, but to date EPA officials have declined to review the study or approve its release. The updated risk assessment reportedly still links exposure to formaldehyde and leukemia, despite the NRC's criticism of that conclusion in 2011. Industry groups have met with EPA and have publicly expressed concerns that the updated risk assessment will be merely a "restructuring" of the original draft and will still suffer from the same scientific and methodological defects previously identified by the NRC. Consumer groups and legislators have accused EPA of bowing to industry pressure to withhold the updated assessment and have continued to call for its release. Meanwhile, EPA has suggested that the agency is re-evaluating some of the science underlying the assessment and is currently facing a lawsuit filed by Public Employees for Environmental Responsibility (PEER) alleging that EPA failed to respond to the group's public records request.

As the debate over the release of the risk assessment heated up earlier this year, EPA was also forced to defend its decision to delay the effective date of a Final Rule implementing the Formaldehyde Emission Standards for Composite Wood Products Act of 2010 (Formaldehyde Final Rule), which amended the Toxic Substances Control Act (TSCA) to add TSCA Title VI. The Formaldehyde Final Rule sets forth emissions limits for formaldehyde in composite wood products (which are often used in furniture, flooring and construction) and imposes a number of testing and record-keeping requirements on companies in the supply chain. Although the Formaldehyde Final Rule was originally scheduled to take effect in December 2017, EPA announced a year-long delay in September 2017 in order to allow companies more time to prepare for compliance.

Consumer groups objected to EPA's decision, citing alleged immediate threats to public health from exposure to formaldehyde. After filing suit against EPA in California federal court, they reached an agreement with EPA that the agency would begin enforcement of the Formaldehyde Final Rule as of June 1, 2018—more than six months earlier than companies had planned. The new June 1 compliance date posed serious compliance challenges and came at great cost to furniture manufacturers, distributors and retailers, who were forced to act quickly to design and implement procedures that were not expected to be required until months later.

For companies in the retail industry, the controversy over formaldehyde has led to greater public scrutiny of the chemical and its alleged health effects, which often translates into increased litigation risk. Plaintiff's lawyers searching for the "next wave" of toxic tort and product liability litigation may look to get out ahead of EPA's formaldehyde risk assessment, filing lawsuits early and banking on the report's anticipated conclusions regarding leukemia. For their part, consumer groups may also put pressure on companies by conducting their own independent studies of popular consumer products and publicizing results that show traces of formaldehyde in those products in an effort to garner public support for new regulations.

The fallout from the formaldehyde controversy is also likely to affect EPA's review and regulation of chemicals in the future. Although TSCA was amended in 2016 by the Frank R. Lautenberg Chemical Safety for the 21st Century Act (Lautenberg Act) to give EPA new powers to review and regulate chemicals at the federal level, EPA does not always act with the expediency or methodology consumer advocacy groups may want. EPA is currently in the process of evaluating 10 "high priority" chemicals as mandated by the Lautenberg Act, and is already facing criticism from consumer groups who do not feel that EPA's framework for those analyses is comprehensive enough. And just as with the formaldehyde risk assessment, it is unlikely that industry groups will universally approve of the conclusions EPA reaches in connection with these new risk evaluations or the methodology it uses.

As EPA's new evaluations progress and are released, we expect to see challenges from both consumer groups and industry groups similar to those launched over formaldehyde. The uncertainty those challenges will create will pose compliance difficulties for even the most proactive companies while regulations are tied up in litigation with unpredictable outcomes. Likewise, the heightened public interest in chemical evaluations means that companies may find themselves facing lawsuits and defending their products in the court of public opinion—even if EPA concludes that certain chemicals pose no significant health risk to consumers.

CALIFORNIA CONSUMER PRIVACY ACT AND ITS IMPACT ON RETAILERS

Lisa Sotto, Aaron Simpson and Brittany Bacon

Lisa is chair of the global privacy and cybersecurity practice and managing partner of the firm's New York office. Aaron and Brittany are partners in the global privacy and cybersecurity practice in the firm's New York office.

The California Consumer Privacy Act of 2018 (CCPA), signed by California Governor Jerry Brown on June 28, 2018, with a compliance deadline of January 1, 2020, signals a shift in the data privacy regime in the US. The CCPA was passed quickly by California lawmakers in an effort to remove a ballot initiative of the same name from the November 6, 2018, statewide ballot. The CCPA likely will require businesses, including retailers, to make significant changes to their data protection programs, if the business has consumers or employees who are California residents.

On September 23, 2018, Governor Brown signed into law SB-1121, which makes limited substantive and technical amendments to the CCPA. SB-1121 takes effect immediately and delays the California attorney general's (AG's) enforcement of the CCPA until six months after publication of the AG's implementing regulations, or July 1, 2020, whichever comes first.

Key provisions of the CCPA include:

- **Applicability.** The CCPA will apply to any for-profit business that: (1) "does business in the state of California"; (2) "collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information"; and (3) satisfies one or more of the following thresholds: (a) has annual gross revenues in excess of $25 million; (b) alone or in combination, annually buys, receives for the business's commercial purposes, sells or shares for commercial purposes, the personal information of 50,000 or more consumers, households or devices; or (c) derives 50 percent or more of its annual revenues from selling consumers' personal information (collectively, Businesses).
- **Definition of Consumer.** The CCPA defines "consumer" as a natural person who is a California resident.
- **Definition of Personal Information.** Personal information is defined broadly as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." The CCPA's definition of personal information also contains a list of enumerated examples of personal information, which includes, among other data elements, name, postal or email address, Social Security number, government-issued identification number, biometric data, Internet activity information and geolocation data, as well as "inferences drawn from any of the information identified" in this definition.
- **Definition of Sale.** The CCPA broadly defines sale as "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration." The law provides several enumerated exceptions detailing activities that do not constitute a "sale" under the CCPA.

- **Privacy Policies.** The CCPA will require certain disclosures in businesses' online privacy notices, including a description of consumers' rights under the CCPA (e.g., the right to opt out of the sale of their personal information). Businesses must also disclose certain data practices from the preceding 12 months about the categories of personal information collected about consumers, the categories of sources from which the personal information is collected, the business or commercial purpose for collecting or selling personal information and the categories of third parties with whom the business shares personal information. If the Business sells consumers' personal information or discloses it to third parties for a business purpose, the notice must also include lists of the categories of personal information sold or disclosed about consumers in the preceding 12 months.
- **Access Right.** Upon a verifiable request from a consumer, a business must disclose: (1) the categories and specific pieces of personal information the business has collected about that consumer; (2) the categories of sources from which the personal information is collected; (3) the business or commercial purposes for collecting or selling personal information; and (4) the categories of third parties with whom the business shares personal information. A Business that sells a consumer's personal information or discloses it for a business purpose must also disclose: (1) the categories of personal information that the business sold about the consumer; (2) the categories of third parties to whom the personal information was sold (by category of personal information for each third party to whom the personal information was sold); and (3) the categories of personal information that the business disclosed about the consumer for a business purpose.
- **Deletion Right.** The CCPA will require a business, upon verifiable request from a consumer, to delete personal information about the consumer which the business has collected from the consumer and direct any service providers to delete the consumer's personal information. There are several enumerated exceptions to this requirement, two of which broadly state that compliance with a deletion request is not required when "it is necessary for the business or service provider to maintain the consumer's personal information" to: (1) "enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business" or (2) "use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information."
- **Opt-Out Right.** Businesses must provide a clear and conspicuous link on their website that says "Do Not Sell My Personal Information" and provide consumers a mechanism to opt out of the sale of their personal information, a decision which the Business must respect.
- **Specific Rules for Minors.** If a business has actual knowledge that a consumer is less than 16 years of age, the CCPA prohibits a business from selling that consumer's personal information unless: (1) the consumer is between 13-16 years of age and has affirmatively authorized the sale (i.e., they have opted in); or (2) the

consumer is less than 13 years of age and the consumer's parent or guardian has affirmatively authorized the sale.

- **Non-Discrimination and Financial Incentives.** Businesses cannot discriminate against consumers for exercising any of their rights under the CCPA. Businesses can, however, offer financial incentives for the collection, sale or deletion of personal information.
- **Enforcement.**
  - The CCPA is enforceable by the California AG and authorizes a civil penalty up to $2,500 for each violation or $7,500 for each intentional violation.
  - The CCPA provides a private right of action only in connection with certain "unauthorized access and exfiltration, theft, or disclosure" of a consumer's nonencrypted or nonredacted personal information, as defined in the state's breach notification law, if the business failed "to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." The consumer may bring an action to recover damages up to $750 per incident or actual damages, whichever is greater.

Due to the CCPA's likely effect on the data protection programs of many businesses that have California consumers or employees, it is imperative that retailers develop a CCPA compliance strategy to determine the extent to which the law applies to them, assess their current CCPA compliance posture and conduct any necessary remediation activities.

> "Recognized as one of the "Law Firms Highly Recommended by Corporate Counsel."

SEC ACTIVITY IN 2018

Scott Kimpel and Hannah Flint

Scott, who formerly served on the Executive Staff of the SEC as Counsel to Commissioner Troy A. Paredes, is a partner in the capital markets practice in Hunton Andrews Kurth's Washington office. Hannah is an associate in the capital markets practice in the firm's Washington office.

2018 brought a number of changes at the Securities and Exchange Commission (SEC). Notably, Commissioners Robert Jackson and Elad Roisman were sworn in during 2018, resulting in the five-person commission's being back at full strength. Consequently, the SEC has moved forward on a number of regulatory initiatives aimed at promoting capital formation by seeking to ease compliance burdens on companies while still ensuring that investor protections remain intact.

Disclosure Modernization and Simplification

The SEC continued to make modernizing and simplifying existing corporate disclosure a priority during 2018. On July 24, 2018, the SEC voted to propose rule amendments intended to simplify and streamline the financial disclosure requirements made in connection with registered debt offerings and subsequent periodic reporting for guarantors and issuers of guaranteed securities, as well as for affiliates whose securities collateralize a registrant's securities. The proposed amendments are intended to make investor disclosure easier to understand, and the SEC is hopeful that the changes will have the effect of increasing the number of public offerings that make use of these kinds of credit enhancements, thereby affording investors protection they may not be provided in unregistered offerings.

On August 17, 2018, the SEC voted to adopt amendments to various public company disclosure requirements it believes are redundant, duplicative, overlapping, outdated or superseded. On balance, the amendments to Regulation S-K and Regulation S-X are more technical in nature than revolutionary, but they will nonetheless require reporting companies to revise and update a number of routine disclosures appearing in periodic reports and registration statements. The full slate of amendments is described in the SEC's adopting release, but the amendments include changes to the Business Section, such as removing the requirements to disclose segment financial information, the amount spent on research and development, the financial information by geographic area and any risks related to, and dependence on, foreign operations, and changes to disclosure related to the description of common equity, changes to the Management Discussion & Analysis, such as removing the requirement to discuss seasonality in interim reports, among other changes. These new disclosure standards took effect on November 5, 2018, and are effective for all SEC filings made on or after that date.

Cybersecurity

The SEC continued its efforts to focus on cybersecurity in 2018. For example, the SEC published cybersecurity interpretative guidance for public companies on February 21, 2018. The new interpretative guidance marked the first time that the five SEC commissioners, as opposed to agency staff, have provided official agency guidance to public companies regarding their cybersecurity disclosure and compliance obligations. The guidance reiterates public companies' obligation to disclose material information to investors, particularly when that information concerns cybersecurity risks or incidents, and provides a number of pointers as to how a public company should undertake a materiality analysis in the context of a cybersecurity risk or incident. It also addresses two topics not previously addressed by agency

staff: the importance of cybersecurity policies and procedures in the context of disclosure controls and the application of insider trading prohibitions in the cybersecurity context.

On October 16, 2018, the SEC issued a report of investigation entitled "Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements." As the latest addition to a growing body of guidance concerning cybersecurity for public companies, the report reminds businesses that the internal accounting controls required under the federal securities laws should take into account the threat of spoofed or manipulated electronic communications. The report focuses on a particular kind of cyber scam known as a "business email compromise." According to the SEC, having internal accounting control systems that account for such cyber-related threats and related human vulnerabilities is vital to maintaining a sufficient accounting control environment and safeguarding assets. The SEC also made clear that having internal controls documented on paper is not enough and that employees must be trained appropriately to implement those controls. In issuing the report, the SEC emphasized that it did not mean to suggest that every company that is the victim of a cyber-related scam is automatically in violation of the internal accounting controls requirements of the federal securities laws. Nevertheless, companies' internal accounting controls may need to be reassessed in light of emerging risks, including risks arising from cyber-related frauds. We expect that internal controls over cyber risks will be the subject of increased scrutiny by the SEC and its staff in the future.

With the issuance of the report, the SEC continues its vigilant focus on cybersecurity threats affecting public companies. Given the highly malicious nature of today's cybersecurity environment, we expect the SEC to continue to play a leading role in regulating the cyber practices of US businesses.

Enforcement

2018 was a busy year for the SEC's Division of Enforcement. The SEC recently announced its enforcement results for fiscal year 2018, reporting 821 enforcement actions filed in 2018, compared with the 754 actions filed in 2017. The actions resulted in total disgorgements and penalties of more than $3.9 billion, returned $794 million to harmed investors, suspended trading in the securities of 280 companies and obtained nearly 550 bars and suspensions.

During 2018, the Division of Enforcement took steps to focus additional resources on two key priority areas: protecting retail investors and combating cyber threats.

- **Focus on the Main Street Investor**. Over half of the 490 stand-alone enforcement actions brought by the SEC in 2018 involved wrongdoing against retail investors. The Division of Enforcement's Retail Strategy Task Force (RSTF), which was formed in 2018, contributed to the Division of Enforcement's retail focus by undertaking a number of lead-generation initiatives involving several issues impacting retail investors, including disclosures concerning fees and expenses and conflicts of interest for managed accounts, market manipulations and fraud involving unregistered offerings.
- **Cyber-Related Misconduct**. Since the formation of the Cyber Unit at the end of fiscal year 2017, the Division of Enforcement's focus on cyber-related misconduct has steadily increased. During 2018, the SEC brought 20 stand-alone cases, including those cases involving initial coin offerings and digital assets. At the end of the fiscal year, the Division of Enforcement had more than 225 cyber-related investigations ongoing.

The Division of Enforcement also undertook a new initiative, the Share Class Selection Disclosure Initiative, in 2018 designed to focus on misconduct that occurs in the interaction between investment professionals and their clients.

Whistleblower Program

The SEC's whistleblower program continued to grow in 2018. In 2018, the SEC awarded more than $168 million to 13 individuals whose information and cooperation assisted the SEC in bringing successful enforcement actions, resulting in more dollars awarded to whistleblowers in 2018 than in all prior years combined. The SEC also made two of its largest whistleblower awards during 2018, a total combined $83 million award shared by three individuals, and an award of almost $54 million shared by two individuals. The SEC also received more whistleblower tips in 2018 than in any other previous year.

Nevertheless, not all violations are of such materiality as to support the large awards discussed above. Thus, it is not a lost cause to believe that many employees will continue to report internally. For that reason, we continue to recommend that companies constantly reevaluate their internal reporting programs and whistleblower hotlines so that they are accessible to employees and encourage internal reporting. In addition, allegations that are reported internally need to be handled properly. Among other things, the whistleblower may be incentivized to communicate with the SEC or other regulators quickly if they do not believe their concerns are taken seriously. In addition, companies must train managers to avoid actions that might be deemed retaliatory. Companies should also review their use of separation and severance agreements to make sure their terms do not run afoul of the SEC's whistleblower rules.

Looking Ahead to 2019

In a speech[1] and related congressional testimony[2] delivered in December 2018, SEC Chairman Jay Clayton summarized a number of regulatory priorities for 2019 that may interest retailers. Clayton anticipates a number of efforts focused on the proxy solicitation and voting process. Of particular note for retailers, Clayton would like to take action on the ownership and resubmission thresholds for shareholder proposals under Rule 14a-8. He also hopes to see greater reform in the oversight and regulation of proxy advisory firms.

As to proxy advisors, he would like to see "clarity regarding the analytical and decision-making processes advisors employ, including the extent to which those analytics are company- or industry-specific." A frequent criticism of proxy advisory firms is their one-size-fits-all approach, and on this point, Clayton observed that "it is clear to me that some matters put to a shareholder vote can only be analyzed effectively on a company-specific basis, as opposed to applying a more general market or industry-wide policy." He also made mention of considering both conflicts of interest at proxy advisory firms as well as ensuring that investors have effective access to company's responses to information in proxy advisor reports.

On the topic of long-term investment, Clayton referenced the ongoing debate regarding the "adequacy and appropriateness of mandated quarterly reporting and the prevalence of optional quarterly guidance, and whether our reporting system more generally drives an overly short-term focus." He encouraged market participants to share their views with the SEC if there are other aspects of SEC regulations that drive short-termism. The SEC recently released a more formal request for public comment on these issues.

Clayton also briefly discussed three other risks the SEC is monitoring: (1) the impact to reporting companies of Brexit, the United Kingdom's exit from the European Union; (2) the transition away from LIBOR as a reference rate for financial contracts; and (3) cybersecurity. For retailers with British operations, the Brexit issue is no doubt a central point of concern. Each of the final two issues may impact all publicly traded retailers' periodic disclosures and other policies and procedures.

Finally, Commissioner Stein's holdover term as a commissioner comes to an end at the end of 2018. With her vacancy in early 2019, President Trump will have the opportunity to appoint a replacement for her.

[1] https://www.sec.gov/news/speech/speech-clayton-120618

[2] https://www.sec.gov/news/testimony/testimony-oversight-us-securities-and-exchange-commission-0

TECH AND THE LAW DON'T ALWAYS SEE EYE TO EYE

Ondray Harris

Ondray, the former director of the Office of Federal Contract Compliance Programs (OFCCP) at the US Department of Labor (DOL), is special counsel on the labor and employment team in Hunton Andrews Kurth's Washington office.

Human resources leaders of retail companies and many in the organizational process world believe that new artificial intelligence (AI) will revolutionize how HR functions. At least for the near future, they are only partly right. In the HR context, AI typically refers to data that is processed by algorithms to make decisions regarding employees. Simply put, the belief in the HR world is that "cognitive computing" will transform HR's decision-making process and improve the retail employee's experience.

Not so fast—AI certainly is promising in our world, but let us look at the law. A retail corporation is always responsible for the decisions it makes regarding employees. That responsibility sometimes turns into legal liability. For example, corporate decisions made that are more adverse to legally protected groups such as women, minorities, veterans or the disabled create legal compliance issues. Compliance problems lead to lawsuits, legal expenses, branding concerns and decreased work output efficiencies.

Yes, humans can be biased even unwittingly. In fact, the Human Resource Professional Association (HRPA) found that even employers who strive to be inclusive may subconsciously favor people like themselves (unconscious bias). Additionally, Harvard's Implicit Association Test (IAT) demonstrates that humans have language biases as well. In the HR world, the rationale for AI is that biases find their way into job descriptions, resume selections and thus the hiring process. So the well-intended thinking is: use algorithms designed to find and eliminated the bias patterns. Using the same rationale, it is believed that AI could also present hiring managers with candidates who may have been screened out by human tendency to favor candidates with similar traits, competencies or use of language.

AI, HR and the Law

As stated, when reading articles from *Forbes*, HR magazines, *Business Journals*, etc., it is clear the writers believe AI is going to revolutionize HR. Notwithstanding, changes in the law and legal requirements are not controlled by technological advancements. In fact, the maxim *natura non facit saltum ita nec lex* (i.e., nature does not make a leap, thus neither does the law) stands for the principle that the law and legal responsibilities—while not static—should not change quickly. Therefore, from the legal compliance and enforcement perspective, those magazines, journals and HR experts are either misguided or are not referring to the near future regarding decisions of hiring, firing, lay-offs, pay, promotions, benefits and other terms and condition of employment. Simply put, if the tools that a retail company uses create disparities of 2 percent or greater, OFCCP & DOL, DOJ and EEOC do not care if the disparities were created by a human or an algorithm. Intent is irrelevant. Disparate impact is all that matters.

> Recognized by *Chambers USA* as one of the top retail groups in the country, 2018

AI is constantly learning. So it can learn a bias/mirror human bias.

Amazon, last week, scraped its internal AI recruiting tool as the tool had a bias/discriminated against women. The program actually penalized in points applications that contained the word "women's." The AI favored men as it learned the tech field is dominated by men. So things that indicated female—such as girls' school, women's college, female sport team, etc., downgraded the applicant. Amazon quickly said the program was never used in an official capacity. Interestingly, in the STEM world, some argue AI biases prove that the biases are determined neutrally and thus accurate and fair. However, this is a dangerous doubling-down approach that will not impress government enforcers or private litigants.

Moreover, there is a "Catch-22" here: leaving decisions concerning hiring, terms and conditions solely up to AI that causes disparities can be argued negligent, but not using technology to improve diversity in your workforce and to decrease pay gaps can also be used against you. In other words, compliance is result orientated. From an enforcement stance, the outcome is all that matters. The HR technology landscape continues to be disrupted by AI, but HR must also balance cognitive tech advancements with legal compliance requirements. Without question, AI has administrative use in terms of speed, e.g., automate business processes and reduce administrative load, and help run an internal audit for pay equity. However, if AI creates a disparity, a corporation's human capital must review and rectify the disparity. Government enforcement agencies will not be lenient because a retail corporation's AI created a disparity as opposed to a person.

CLIENT RESOURCE: GC HOT TOPICS MEMO

Hunton Andrews Kurth has introduced a new and 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.

"SHAKY" SCIENCE AND NEW THEORIES OF GLYPHOSATE LIABILITY POSE SIGNIFICANT RISK TO RETAIL COMPANIES

Lori Jarvis, Elizabeth Reese and Emily Mordecai

Lori is a partner and Elizabeth and Emily are associates in the product liability and mass tort litigation practice in Hunton Andrews Kurth's Richmond office.

Glyphosate, the world's most widely used herbicide, has dominated headlines over the last year as Monsanto has battled thousands of lawsuits brought by consumers who claim that the chemical causes cancer. Now, other companies in the retail supply chain are beginning to feel pressure as consumer groups and plaintiffs' lawyers turn their attention to other, less obvious targets after early success against Monsanto in both state and federal courts. But as the potential pool of defendants has expanded, so too has the disconnect between the plaintiffs' success in court and the scientific and regulatory landscape, suggesting that reliance on science will do little to mitigate the risk and cost of glyphosate litigation for companies in the retail industry.

Although the scientific and regulatory communities have disagreed about the alleged carcinogenicity of glyphosate for years, the debate drew little attention from the general public until August 2018, when a California state jury slammed Monsanto with a $289 million verdict after a groundskeeper claimed that his exposure to Roundup® weed-killer caused his non-Hodgkin's lymphoma, in *Johnson v. Monsanto*.[1] While the *Johnson* court later slashed the punitive damages award by $211 million on due process grounds, it ultimately left the jury's causation findings intact and the reduction in damages has done little to quell the media attention on glyphosate.

The International Agency for Research on Cancer (IARC)—a subdivision of the World Health Organization—first classified glyphosate as "probably carcinogenic to humans" in 2015. Two years later, in December 2017, the United States Environmental Protection Agency (EPA) released a risk assessment classifying glyphosate as "not likely to be carcinogenic to humans." A majority of regulators around the world have since sided with EPA, including multiple European agencies, Australia and New Zealand. While California had initially placed glyphosate on its Prop 65 list of chemicals "known to the state to cause cancer" in July 2017 just before EPA released its risk assessment, a federal court temporarily enjoined the state from requiring companies to place Prop 65 warning labels on foods that may contain traces of glyphosate in February 2018, finding that requiring labels would violate the First Amendment because, aside from IARC, "almost all other regulators have concluded that there is insufficient evidence that glyphosate causes cancer."[2] The federal court presiding over the Roundup multidistrict litigation (MDL) has also weighed in on the controversy, calling the testimony of plaintiffs' scientific experts "shaky," but ultimately admissible under the *Daubert* standard.[3]

While retail companies may believe that they have science on their side, the *Johnson* verdict and federal MDL *Daubert*

[1] *Johnson v. Monsanto Co.*, No. CGC16550128 (Cal. Super. Ct., County of San Francisco Aug. 10, 2018).

[2] *See Nat'l Assoc. of Wheat Growers v. Zeise*, 309 F.Supp.3d 842 (E.D. Cal. 2018).

[3] *See* Pretrial Order No. 45: Summary Judgment and *Daubert Motions*, *In Re: Roundup Products Liability Litigation*, No. 16-md-02741-VC (N.D. Cal. July 10, 2018).

decision make clear that that argument may not be enough to win in court. Companies will be forced to defend against the narrative crafted by plaintiffs' lawyers and consumer advocacy groups like the Environmental Working Group (EWG), who have worked to keep glyphosate in the public eye by criticizing prominent companies for alleged glyphosate residue in their products and calling for tougher regulations. EWG has emerged as an early leader in glyphosate consumer advocacy, publishing a self-commissioned "study" five days after the *Johnson* verdict that reportedly found that the majority of the food samples tested by EWG contained glyphosate levels higher than what EWG considers to be safe—although none of the products exceeded current legal limits. EWG followed up with a second round of tests in October 2018, claiming that it detected traces of glyphosate in 28 samples of different oat-based food products. EWG has also teamed up with eight major food companies to petition EPA to reduce the current glyphosate tolerance level in oat-based products from 30 ppm to 0.1 ppm, the original level set by EPA in 1993. Most recently, EWG attacked the Food and Drug Administration (FDA) after the agency released a report in October 2018 concluding that over 99 percent of United States-sourced foods it tested in 2016 complied with federal glyphosate tolerance levels. EWG criticized the FDA for not testing oat- and wheat-based products—the type of products EWG claims are most likely to be contaminated by the chemical.

Spurred by their early success against Monsanto and armed with the support of consumer groups like EWG, plaintiffs' lawyers are now looking to target a wider range of defendants, especially those whose products may contain ingredients treated with glyphosate. At least two different companies have been hit with putative class action suits based, at least in part, on the results of EWG's study. Six days after the *Johnson* verdict, **General Mills** was hit with a putative class action suit in Florida, relying on EWG's report in alleging that General Mills deceived consumers by failing to disclose that Cheerios products contain traces of glyphosate.[4] The new claims against General Mills came just as the company agreed to remove the phrase "natural" from its granola products to settle a two-year-old lawsuit alleging that the "100% Natural Whole Grain Oats" label misled consumers because the products contained traces of glyphosate.[5] Another putative class, also citing EWG's report, recently sued **Kellogg Co.** in California for failing to disclose traces of glyphosate allegedly contained in two of its popular food products.[6]

We expect plaintiffs' lawyers to continue to bring glyphosate-related claims against an increasing range of defendants in the retail industry in 2019, which will bring a number of milestones in glyphosate litigation and regulation. The first bellwether trials of the Roundup federal multidistrict litigation are scheduled to begin in February and May 2019, and Monsanto's appeal of the *Johnson* verdict will work its way through the courts.

Because glyphosate is so widely used in agriculture, it is likely that plaintiffs' lawyers have only scratched the surface of the potential pool of glyphosate defendants, which could include any company in the retail chain associated with a product with components that may have been treated with glyphosate at some point in the manufacturing process. Companies that advertise their products as "natural" or "organic" or tout their products' health benefits should be especially aware of the threat of glyphosate litigation, especially because plaintiffs' lawyers tend to bring those types of claims as nationwide class actions. And all companies should take the opportunity now—before being hit with litigation—to review supply and distribution agreements to evaluate and negotiate risk-shifting and indemnification provisions associated with products that may be the subject of glyphosate litigation.

[4] *See Doss v. General Mills Inc.*, No. 0:18-cv-61924 (S.D. Fla. Aug. 16, 2018).

[5] *See Organic Consumers Association, et al. v. General Mills, Inc.*, No. 2016 CA 006309 B (D.C. Super. Ct. Sept. 21, 2018).

[6] *Kien v. Kellogg Co.*, No. 3:18-cv-02759-AJB-MSB (S.D. Cal. Dec. 7, 2018).

MERGERS AND ACQUISITIONS IN 2018

Scott Kimpel and Candace Moss

Scott, who formerly served on the Executive Staff of the SEC as Counsel to Commissioner Troy A. Paredes, is a partner in the capital markets practice in Hunton Andrews Kurth's Washington office. Candace is an associate in the mergers and acquisitions practice in the firm's Washington office.

Overview

In the first nine months of 2018, global M&A activity hit a record of $3.3 trillion, which represents an increase of 37% compared to the same period in 2017. However, the number of deals declined by 9% compared to 2017, representing the lowest deal volume in three years. Based on target industry, the consumer products and services industry and the retail industry each represented 4% of total worldwide announced M&A.[1]

According to reports by PwC, for US consumer markets M&A activity through Q3 2018 there was a year-over-year decrease in deal volume of 11.9%, but an increase in total deal value of 11.8%. Based on sector category within consumer markets, for the consumer sector, there was a decrease in total deal value of 23.1% and a decrease in total deal volume of 20.5% compared to the same period in 2017. The retail sector experienced a decline in total deal volume of 18.2%, while total deal value remained relatively flat with a slight decrease of 1.7%. Year-to-date as of the end of Q3 2018, the top three consumer markets subsectors based on announced deal value were food and beverage ($55.6 billion), other consumer products (including products such as appliances, furniture and consumer electronics) ($24.7 billion) and grocery, drug, discount and mass ($23.3 billion). The top three subsectors based on the number of announced deals were other consumer products (228 deals), food and beverage (208 deals) and specialty retail/other (including electronics, home improvement, auto repair and other categories) (186 deals). In Q3 2018, smaller transactions of $50 million or less became increasingly popular, with such transactions accounting for 61% of total deals, compared to 54% of deals in Q2 and 59% of deals in Q1.[2]

Looking Ahead to 2019

Although M&A activity continues to be strong, factors such as global trade policy, rising interest rates and market volatility could affect deal volume in 2019. The trade war between China and the United States, continued threats by President Trump to withdraw from NAFTA before the newly signed United States-Mexico-Canada Agreement takes effect in 2020, and the impending Brexit all threaten to negatively impact M&A, particularly cross-border deals. Additionally, interest rates have been rising and are expected to keep climbing, which could increase the cost of capital for transactions. Stock markets experienced volatility at various points throughout 2018, with the Dow Jones Industrial Average not only closing at a record high and having the third-largest one-day point gain in its history, but also experiencing the

[1] http://dmi.thomsonreuters.com/Content/Files/3Q2018_MA Legal_Advisor_Review.pdf

[2] https://www.pwc.com/us/en/industries/consumer-markets/assets/pwc-us-consumer-markets-deals-insights-q3-2018.pdf; https://www.pwc.com/us/en/industry/assets/pwc-us-consumer-markets-deals-insights-q2-2018-final.pdf; https://www.pwc.com/us/en/consumermarkets/assets/pwc-us-consumer-markets-deals-insights-q1-2018.pdf

four largest daily point losses on record.[3] Although some of the volatility has been attributed to fears surrounding the US/China trade war, after a long bull market, there is also some speculation whether the next bear market may be afoot.

Despite the economic uncertainty created by the aforementioned and other factors, a Deloitte 2019 M&A trends report shows that there is still a healthy appetite for M&A heading into 2019, with 76% of domestic corporate M&A executives and 87% of domestic private equity M&A executives expecting the number of M&A deals to increase over the next year, and 70% of executives expecting an increase in average deal value. Many executives expect that rising interest rates may lead to an accelerated pace of M&A activity in 2019, in order to close deals before interest rates increase further.[4] Notwithstanding some unfavorable global trade policy developments, corporations and private equity firms still view Canada and China as the top most likely international markets for M&A. The lingering impact of tax reform and increased corporate savings could also encourage deal activity. Overall, while at first glance market conditions may appear to be poised to slow down M&A activity, there is reason to remain optimistic that there will not be an immediate sharp decline, as companies and private equity firms still seek to engage in strategic transactions.

[3] https://www.cnn.com/2013/05/31/us/dow-jones-industrial-average-fast-facts/index.html; https://markets.businessinsider.com/news/stocks/dow-jones-stock-market-news-today-trump-china-march-26-2018-3-1019458619; https://www.businessinsider.com/largest-stock-market-drops-in-history-2018-2; https://www.cnbc.com/2018/12/04/stock-market-dow-futures-fall-amid-us-china-trade-deal-skepticism.html

[4] https://www2.deloitte.com/us/en/pages/mergers-and-acquisitions/articles/ma-trends-report.html

> “...the [retail] team provides a holistic service, not matter by matter, which has helped us gain a better competitive position.” – *Chambers USA*, 2018

‘BRICK AND MORTAR’...OR ‘BRICK AND MOBILE’?

Cecilia Oh and Hunter Glenn

Cecilia is a partner and Hunter is an associate in the outsourcing, technology and commercial contracting practice in the firm’s Washington and Richmond offices, respectively.

Brick-and-mortar retailers are rapidly diversifying their shopping, checkout and payment methods in an effort to combat the erosion of sales to online channels and to provide an improved experience for their consumers. As a result, when a customer enters a store, they may encounter everything from self-checkout kiosks to store-specific mobile applications, scan-as-you-go devices or even sales clerks toting smartphones that can complete the transaction in the middle of an aisle. Recently, however, more and more retailers have been making plans to implement the “just walk out” model, which allows consumers to, quite literally, just walk out with their items once they are done shopping.

In these cashierless stores, consumers scan their smartphone app to enter. Then, the customer may browse the aisles as they typically would. As the buyer shops, the store, using the same type of technology and sensors employed by self-driving cars, identifies the shoppers, their items and what products are moving off the shelves. Once the consumer has finished, they are free to exit, and their purchase is billed to their account with the retailer.

It is no wonder that these models are becoming increasingly popular, as it is attractive to both consumers and retailers alike. In fact, it is so attractive that, by some estimates, these automated technologies could account for 35 percent of retail sales in the next 20 to 30 years. From the consumer’s perspective, grab-and-go retailers offer a streamlined process and allow buyers to quickly enter a store, grab what they need and get back to their daily routine, without having to wait in a long checkout line. This “friction free” shopping experience is designed to entice consumers to get out and shop more, thereby increasing not only the frequency of in-store visits, but, ultimately, sales volumes. Studies have long hypothesized that credit cards and cashless transactions encourage consumers to spend more, boosting the store’s profits.[1]

For the retailers, using these models is attractive for a number of reasons, including helping to lower labor costs due to the smaller number of employees required to maintain the store. The smaller labor force also offers the potential for the store to expand its business hours, without increasing safety concerns for employees working the late-night shift. The lack of cash kept on the premises, along with the store’s wide use of video cameras and other authentication technology, could make a store less attractive for certain types of crime that frequently occur at brick-and-mortar stores, such as a theft and robbery. Additionally, these models help avoid the administrative and logistical troubles that can accompany keeping cash in a store including accounting, running cash back and forth to the bank and ensuring registers are stocked. According to one estimate, “such hassles cost retailers an average 9.1 percent of sales, ranging from 4.7 percent at grocery stores to 15.5 percent at restaurants and bars...compare[d] to the 2 to 3 percent transaction fees credit-card companies charge merchants.”[2] Finally, though the consumer might feel like a shoplifter as they adapt to the process, because of the sophisticated software tracking the store’s goods, the grab-and-go model also helps to prevent theft.

[1] https://www.nytimes.com/2016/03/27/your-money/credit-cards-encourages-extra-spending-as-the-cash-habit-fades-away.html

[2] https://www.usatoday.com/story/money/2018/11/28/holiday-shopping-more-retailers-just-saying-no-cash/2063747002/

However, these benefits are not without their own set of risks. There is a wide range of potential issues that retailers should consider before launching their own cashierless technology, including the following:

- increases in interchange rates if these transactions (which would otherwise be considered "card present") are interpreted as "card not present" exchanges;
- claims of discrimination by certain classes of people who are unable to fully access these technologies (e.g., persons with disabilities and those without access to mobile devices, bank accounts or other prerequisites);
- labor disputes arising from the elimination of jobs;
- consumer privacy concerns (e.g., invasion of privacy claims in connection with the tracking of customers' browsing, risks associated with the collection and processing of high volumes of intimate personal data and unexpected behavior of artificial intelligences);
- compliance with regulations governing authentication technologies and other security controls (e.g., use of biometrics to authenticate customers entering retail locations);
- compliance with regulations involving the sale of age-restricted goods (e.g., alcohol, tobacco, firearms, etc.);
- loss management and fraud detection issues, including the allocation of liability among technology vendors in connection with technology failures;
- other issues relating to relationships with technology vendors, including ownership of customer relationships and customer data, data use restrictions and participation in future revenues resulting from retailer contributions to the development and "training" of artificial intelligence engines;
- protection of intellectual property, including patents, trademarks and data;
- whether existing insurance policies adequately address this changed business model; and
- all of the more typical issues associated with procuring and deploying new technologies, such as technology use rights, implementation plans and costs, service levels, business continuity requirements and warranties, indemnities and limitations of liability.

There is no doubt that there is a revolution coming to the way consumers buy goods at brick-and-mortar stores. These new strategies help retailers better meet customers' need for speed, create novel shopping experiences and incorporate technology into their stores. However, as retailers begin to put their own touch on this new approach to commerce, they should be sure to consider the potential risks that may accompany the new technology.

LANDMARK CASE BEFORE ILLINOIS SUPREME COURT COULD STEER FUTURE OF BIOMETRIC-DATA PROTECTION LITIGATION AND LEGISLATION IN THE UNITED STATES

Torsten Kracht, Lisa Sotto and Bennett Sooy

Torsten is a partner in the commercial litigation practice in Hunton Andrews Kurth's Washington and New York offices. Lisa is chair of the global privacy and cybersecurity practice and managing partner of the firm's New York office. Bennett is an associate in the competition and consumer protection practice in the firm's Washington office.

The Illinois Biometric Information Privacy Act (BIPA) is currently the most important statute in the US concerning the collection and storage of biometric data. This past year saw a continuing escalation of putative class cases filed under the law, both inside and outside of Illinois, due to BIPA's express private right of action and per-violation statutory penalties of $1,000 or more. The vast majority of these cases involve the use of devices by retailers that capture biometric data such as fingerprints or iris images for the purpose of tracking customers and tracking employee attendance or cash-register access. Other biometric devices of immediate relevance to retailers and BIPA are store security systems that use facial recognition technologies.

To date, courts applying BIPA have been proceeding without a definitive interpretation of the nature of the harm required to demonstrate a violation of the BIPA. Is it enough for a defendant to have gathered biometric information in violation of the act, or does there have to be actual harm such as a data breach pursuant to which the biometric information is compromised and used for criminal purposes?

For the first time since the passage of BIPA in 2008, the Illinois Supreme Court is set to answer the question of whether persons "aggrieved" by a violation of the statute must allege that they suffered actual harm or if a technical violation of the statute is sufficient to establish standing. What the court decides has the potential to spur national biometric litigation along even further or render BIPA toothless; it will also directly affect how other states draft their biometric-data protection statutes.

The court heard oral argument on November 20, 2018, in ***Stacy Rosenbach v. Six Flags Entertainment Corp, et al.***, No. 123186 (Ill.), regarding the nature of the harm required to sue under BIPA. The plaintiff in the case has asserted a claim based on a technical violation of the statute: her son's fingerprint scan was collected by the amusement park in order to access a season's pass, but the park failed to comply with the notice and consent requirements of BIPA. The defendants pressed the point that interpreting BIPA to allow private enforcement of technical violations has opened the floodgates to "no-injury lawsuits," and argued that while a company that fails to comply with BIPA's notice-and-consent requirements is liable if the information it collects is compromised or misused in violation of the law, collection alone fails to trigger liability.

During oral argument, several justices seemed to side with the plaintiff, citing collection of biometric data itself without notice and consent as a potential "irreparable harm" and noting that the purpose of the statute was to prevent actual harm from happening in the first place. We anticipate that the Illinois Supreme Court will issue its opinion in Q1 2019.

Interestingly, BIPA was originally enacted in reaction to a situation that presents a cloudy issue as to actual versus potential harm. When Pay By Touch, a biometrics firm that supplied fingerprint scanners to Illinois retailers, faced bankruptcy in 2007, the company considered selling its database of fingerprints collected by the scanners. The Illinois chapter of the American Civil Liberties Union used the opportunity to draft BIPA, which was passed by the Illinois legislature the next year.

The idea of a corporation's selling a person's biometric information collected without notice to or consent of the individual certainly leaves a bad taste in the mouth of most people, but is it actually harmful? For that reason, most courts thus far have interpreted BIPA as vesting in Illinois residents the right to control their biometric information by requiring notice before collection and providing residents with the crucial ability to withhold consent. There are, however, some courts which have required a showing of actual harm for litigants to have standing to bring a claim under BIPA.

A decision by the Illinois Supreme Court holding that a plaintiff has standing to enforce BIPA based on only a technical violation of the statute would keep the tide of national biometric collection litigation rolling. Although Texas and Washington have their own statutes governing the collection and usage of biometric identifiers, those laws do not allow for private actions. BIPA has been the main vehicle in biometrics-related (especially class action) litigation due to its private right of action and steep statutory penalties.

BIPA is likely to remain the relevant benchmark for legislation controlling the collection of biometric information as efforts to pass a bill at the federal level have not been successful. In the House, the Biometric Information Privacy Act (H.B. 4381) was introduced in 2014 and requires permission before entities can share biometric data they collect with a third party, but no action has been taken on this bill to date. Additionally, the Secure and Protect Americans' Data Act (SPADA) and the Data Accountability and Trust Act (DATA) both include biometric data as a protected category of personal information for which entities that collect it must provide notice, but no action has occurred on either bill since their proposal in 2017. In the Senate, the Customer Online Notification for Stopping Edge-provider Network Transgressions Act (CONSENT Act) and the Social Media Privacy Protection and Consumer Rights Act (SMPPCR Act) were both proposed in 2018 and potentially cover biometric information under their definitions of "personally identifiable information" and "personal data," respectively, but no action has been taken to date on either bill.

> "Working with Hunton Andrews Kurth has led to transformational outcomes for our business and legal departments." – *Chambers USA*, 2018

ENHANCED PRACTICE GROUP CAPABILITY: RETAIL LITIGATION IN THE INTERNATIONAL TRADE COMMISSION

Aimee Soucie, John Flock and Paul Qualey

Aimee, John and Paul are partners in the intellectual property practice in Hunton Andrews Kurth's Washington, New York and Washington offices, respectively.

The merger of Hunton & Williams and Andrews Kurth Kenyon in 2018 resulted in an intellectual property (IP) group with a long, successful history of handling high-stakes Section 337 investigations at the US International Trade Commission (ITC). Our attorneys from Kenyon & Kenyon first became familiar with the venue in the 1970s and were soon after joined in the 1980s by a former chief administrative law judge of the ITC, who helped develop the skilled practice that continues at our combined firm today.

The Hunton Andrews Kurth ITC team has been involved in precedent-setting investigations. For decades, we've authored the leading treatise on navigating IP litigation in the ITC, "Unfair Competition and the ITC: A Treatise on Section 337 Actions" (published by Thomson Reuters). And, more than a third of the attorneys in our IP group—including attorneys originating from Hunton, Andrews Kurth, and Kenyon—have worked on multiple ITC investigations. With clients ranging from Global Fortune® 100 corporations who trust us to represent them in ITC litigation year after year to businesses engaging us for the first time, we have represented US-based and international companies in over 50 Section 337 investigations during the past 10 years alone, on both the complainant and respondent sides.

ITC 101

While Section 337 of the Tariff Act of 1930, as amended, is a trade statute that addresses unfair acts involving the importation into and sale in the United States of "articles," those unfair acts include infringement of IP rights by retail goods. The ITC conducts investigations to resolve disputes regarding alleged patent, trademark and copyright infringement, and other allegations of unfair competition, such as trade secret misappropriation and false advertising, with respect to products that are imported into, sold for importation into and/or sold in the United States after importation from abroad.

Section 337 investigations are known for their speed, complexity and the powerful threat of an exclusion order preventing the entry (and sale) of products into the United States; the ITC does not award monetary damages. From institution to a final determination by the Commission, most investigations conclude in 14 to 16 months, with a hearing on the merits a mere seven to nine months after a complaint is filed. On top of that, an ITC investigation includes proofs not required or considered in district court, such as importation, domestic industry and the public interest.

The ITC is a Popular Forum for Consumer Electronics and Patent Infringement Allegations

Section 337 investigations are well known as investigations into allegations of utility patent infringement made against retailers and manufacturers of popular consumer electronics, such as mobile phones, tablets, televisions, digital cameras and gaming systems.

That reputation is not undeserved.

Of the 12 ITC matters handled by Hunton Andrews Kurth over the past 18 months, almost half related to accused products falling within that category, and all involved patent infringement allegations.

In 2018, similar types of ITC investigations were brought against other consumer electronics companies, such as Apple, Comcast, DJI, HP, HTC, Lenovo and Nintendo.

But the ITC is Also Useful for Other Retail Products and Types of Unfair Competition

Of interest to the retail industry, there are many different types of products, companies and allegations investigated by the ITC. For example, this year, the ITC instituted investigations related to the automotive sector (infotainment systems, motorized "off-road" vehicles, fuel vapor canister systems); sports equipment (jump rope systems, archery equipment, strength-training systems); home and office goods (convertible sofas, printer toner cartridges, height-adjustable desk platforms); and food and beverages (beverage containers, beverage dispensing systems, microperforated packaging for fresh produce, water filters, electronic nicotine delivery systems). Parties to these investigations ranged from complainants Anheuser-Busch, Bear Archery, Canon, Electrolux, Fiat Chrysler Automobiles, Hoist Fitness Systems, Juul and Varidesk , to respondents Denso, Glory Foods and Growers Express, Heineken, Krug, Mahindra, Panasonic and Toyota . Some of these investigations included allegations of design patent infringement, trademark infringement and trade dress misappropriation. In the recent past, the ITC has investigated similar allegations of infringement and misappropriation, as well as counterfeiting, in the fashion industry, including based on complaints brought by Converse, Crocs and Louis Vuitton.

*****

In short, as a member of the retail industry, whether you are accused of violating Section 337 or are seeking to secure exclusion and cease and desist orders against an infringer of your IP rights, we will use our vision, wisdom and drive to vigorously defend and protect the interests of your company. Our attorneys have the specialized expertise and comprehensive understanding of the unique challenges presented by litigating in the ITC necessary to succeed in these investigations.

KEY CONTACTS

Robert Quackenboss
Partner, Washington

+1 202 955 1950 | rquackenboss@HuntonAK.com

Bob is the editor of the *2018 Retail Industry Year in Review*. He represents businesses in resolving their complex labor, employment, trade secret, non-compete and related commercial disputes.

Randy Parks
Partner, Richmond

+1 804 788 7375 | rparks@HuntonAK.com

Randy is co-chair of the firm's corporate team, chair of the global technology and outsourcing practice group, co-chair of its retail and consumer products industry practice group and serves on the firm's executive committee. His practice focuses on global technology, outsourcing and complex commercial transactions.

Steve Patterson
Partner, Washington

+1 202 419 2101 | spatterson@HuntonAK.com

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

ABOUT US

Hunton Andrews Kurth is a global law firm of more than 1,000 lawyers handling transactional, litigation and regulatory matters for clients in myriad industries including energy, financial services, real estate, retail and consumer products 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 200 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.

HUNTON
ANDREWS KURTH

HuntonAK.com