NFP

H1 2023

Midyear Claims Journal

Financial Services and Management Liability

Table of Contents

Financial Institutions

The first half of 2023 saw a significant amount of legal and regulatory action, driven in no small part by the rapid failures of three large regional banks. Even without the quick collapse of Silicon Valley Bank and others, the first half of 2023 was ripe with action as federal and state regulators continued to push stronger regulatory enforcement.

> There were also **several notable** cases these first **six months**, including a **$1B security** class action **settlement**.

We summarize these major legal trends below, while also briefly outlining several issues on the horizon for the back half of this year.

Silicon Valley Bank Fallout

The legal and regulatory response to the collapse of Silicon Valley Bank (SVB), Signature Bank and First Republic Bank in March was almost immediate. Dozens of lawsuits will play themselves out in the court system over the next several years, and proposed regulatory rulemaking may take equally as long. In the meantime, it is likely that the most immediate impact will be felt through the regulatory supervisory process of various federal and state agencies.

Class Action Suits Filed

Multiple proposed class action lawsuits were filed almost immediately following the banks' failures. These include suits against bank executives and underwriters. Goldman Sachs, Bank of America and Morgan Stanley were among the underwriters sued in relation to the SVB collapse. Plaintiffs alleged in their complaint that along with SVB executives, the defendants "concealed the magnitude of the risks facing the Company's business model that would result from any decision by the Federal Reserve System raising the federal funds rate." *City of Hialeah Employees' Retirement System v. Becker et al, Case No. 23-cv-1297 (N.D. Cal. April 7, 2023)*.

Suits were also filed against auditors, accountants and consultants. In one such suit, Credit Suisse shareholders filed a proposed class action against Credit Suisse executives and the global auditing firm KPMG. The complaint alleges that KPMG and its partners allowed a "common course of misconduct and civil conspiracy" to go unchecked for over a decade at the bank, ultimately leading to Credit Suisse's collapse. The complaint also alleges violations of the Racketeer Influenced and Corrupt Organizations (RICO) Act and breaches of statutory duties. *Stevenson v. Thornburgh et al., Case No. 23-cv-04458 (S.D.N.Y. May 28, 2023).*

Regulatory Response

The regulatory response was also immediate, although long-term consequences remain to be seen. Lawmakers and federal regulators questioned how these large regional banks collapsed. In short order, the Federal Reserve, FDIC, New York State Department of Financial Services, and the Government Accountability Office all released reports in late April regarding the failures of SVB and Signature Bank. Congress also responded, raising concerns from the mismanagement of bank executives to questioning why bank customers kept billions in oversized deposits in the banks.

The Swiss government also responded. It ordered Credit Suisse to cut or reduce bonuses for approximately 1,000 senior bankers. This will save up to $66.3 million, as any outstanding bonuses for the executive board will be cancelled and bonuses for members below executive level will be reduced by half to a quarter.

Back in the US, while any new changes through rulemaking by either lawmakers or banking regulators could potentially take years and face legal challenge, we anticipate that we will continue to see an increase in the regulatory supervisory and enforcement process as well as more scrutiny during routine exams.

Increased Regulatory Scrutiny

Our belief in further regulatory scrutiny through exams and enforcement process is in line with the approach federal regulatory agencies have taken in the first half of 2023. In notable news, the SEC challenged major crypto players and signaled an escalation of its efforts to rein in the digital asset industry. The Federal Reserve, FDIC and the Office of the Comptroller of the Currency (OCC) released new policies and guidance that hint at stronger bank enforcement actions. And Colorado is attempting a first-in-kind legislation to rein in online banking.

SEC Challenges Cyrptocurrency

In early June, the SEC sued two of the largest crypto companies. On June 5, the SEC brought suit against Binance Holdings Ltd., the world's largest crypto platform, and its founder, Changpeng Zhao. The SEC alleged that Binance had blatantly disregarded federal securities laws and, in doing so, enriched themselves by billions of dollars while placing investors' assets at significant risk. The complaint further stated that the defendants purposefully planned to evade US regulatory oversight. In a related statement, SEC Chairman Gary Gensler stated that "Zhao and Binance entities engaged in an extensive web of deception, conflicts of interest, lack of disclosure and calculated evasion of the law." *SEC v. Binance Holdings Ltd., Case No. 23-cv-1599 (D.D.C. June 5, 2023)*.

The following day, the SEC sued Coinbase Inc., the largest crypto exchange in the US, alleging that it operates as an unregistered crypto-asset trading platform. According to the SEC complaint, Coinbase services over 100 million customers and accounts for billions of dollars in daily trading volume in hundreds of crypto assets. The SEC alleged that Coinbase has operated as an unregistered broker, exchange and clearing agency since at least 2019. The complaint further states that:

> By collapsing these functions into a single platform and failing to register with the SEC as to any of the three functions, and not having qualified for any applicable exemptions from registration, Coinbase has for years defied the regulatory structures and evaded the disclosure requirements that Congress and the SEC have constructed for the protection of the national securities markets and investors. *SEC v. Coinbase, Case No. 23-cv-4738 (S.D.N.Y. June 6, 2023)*.

The SEC also this year has begun labeling dozens of cryptocurrencies as securities in order to bring them under SEC control. It has also warned broker-dealers and investment advisors to use "heightened scrutiny" when advising clients on risky or complex products for clients, including crypto assts, and determining whether they are in the investor's best interest.

Through these escalating actions, the SEC is targeting the digital asset industry. Whether the courts or Congress intervene to enact regulations for these crypto markets will be one of the key events to watch for in the back half of this year.

Federal Regulators' New Warning and Guidance

Federal banking regulators were also busy this first half of the year. On May 25, the OCC issued a revised version of its manual regarding bank enforcement actions. The policy and procedure manual revisions could be viewed as a potential warning for increasingly severe enforcement measures against banks that exhibit "persistent weaknesses."

The Federal Reserve, FDIC, and OCC also jointly issued a unified set of risk management guidance for third-party bank risks on June 6. Banks have increasingly engaged in third-party relationships related to technology, professional services, and other business and outsourcing relationships in an effort to expand customer offerings. The use of third parties can offer banking organizations significant benefits, such as quicker and more efficient access to technologies, human capital, delivery channels, products, services and markets.

However, as these third-party relationships proliferate, so do the potential risks. These can include operational disruptions, compliance violations, strategic risk, cybersecurity incidents and, potentially, financial losses.

> The joint guidance states that banks must "**identify**, **assess**, **monitor** and **control**" these relationships, and sound **third-party risk management** takes into account the level of risk, complexity, and size of the banking organization and the nature of the **third-party relationship**.

The three regulators issued the joint guidance to "promote consistency in supervisory approaches," and it replaces each agency's existing general guidance.

Colorado Attempts First of Its Kind Bank Legislation

Colorado recently became the first state to opt out of federal banking laws that allow state-chartered banks – mostly online banks and fintech firms – to lend nationally at the maximum interest rates allowed in their home states, regardless of the local usuary law limits.

> By **opting out** of this federal law, Colorado is attempting to **stop high-cost lending** by out-of-state banks and **force** all banks doing business in Colorado to **abide** by the **Colorado interest rate limits**.

It remains to be seen whether other states will follow and if this new law will withstand legal challenge. Fintech firms and other online banks may also pull out of the state altogether, which would potentially have the opposite effect by decreasing competition for Colorado citizens.

Other Notable Litigation From H1

Quickly rounding up several notable pieces of litigation from the first half of this year, we saw a top 20 security class action lawsuit and multiple insurers winning COVID-19 coverage cases.

Wells Fargo recently agreed to pay $1B to settle a security class action suit that alleged the bank misrepresented its compliance with consent orders issued in 2018 following the fake customer account scandal. The plaintiffs alleged that after the consent orders were issued, the bank and its senior executives misrepresented their compliance and disregarded the consent order requirements. The $1B settlement ranks in the top 20 largest US security class action settlements. The settlement is in addition to the $1B fine Wells Fargo paid to federal banking regulators, customer class actions and other shareholder suits. In *Re Wells Fargo & Company Securities Litigation, Case No. 20-cv-04494 (S.D.N.Y. 2020).*

Insurers continue to win COVID-19 coverage cases, and now appeals, as the cases move their way through the appellate system. In one recent illustrative case, the Ninth Circuit agreed with AIG that a contaminant exclusion barred coverage for all claims related to COVID-19. The court found that the spreading of COVID-19 particles, including by expulsion from infected persons, fits squarely within the ordinary plain meaning of "dispersal" of a "virus." The court held that the plain language of the exclusion makes clear that coverage is barred if the claimed "loss or damage" has any causal connection to the dispersal of a virus. *TP Racing LLLP v. American Home Assurance Co, Case No. 21-16910 (9th Cir. June 1, 2023).*

In an interesting case regarding the push-pull between advancing technology and financial institutions, a JPMorgan Chase customer sued the bank over a Zelle glitch. Zelle, the digital-payment provider, had a technical issue that resulted in double-debiting from Chase accounts although the recipient only saw a single payment. The named plaintiff did not have enough funds in his Chase account to cover two withdrawals, causing an overdraft of his account.

The issue was fixed within thirty-six hours, but plaintiff still had to pay the overdraft charges. The purported class action complaint alleges that JPMorgan Chase is liable for its failure to implement protocols to detect such technical issues and the bank's negligence caused the plaintiffs harm. *Stoll v. JPMorgan Chase Bank NA et al., Case No. 23-cv-04149 (E.D.N.Y. 2023).*

Federal prosecutors recently charged six people in New York with pandemic relief loan fraud related to the Paycheck Protection Program (PPP). In total, the fraudulent PPP applications sought over $14.7M from various financial institutions. The six defendants allegedly submitted 114 fraudulent PPP applications to various financial institutions, seeking loans for 56 different individuals. Thirty-nine of the applications were approved by the various financial institutions, resulting in disbursements totaling more than $4.6M. All defendants are charged with conspiracy to commit wire fraud and two were charged with aggravated identity theft. *USA v. Walker, Case No. 23-mh-04465 (S.D.N.Y. 2023).*

What We're Watching For the Second Half of 2023

There are several notable cases and regulatory decisions that will likely be issued in the back half of this years. Here are the ones we're most closely watching.

Environmental, social and governance (ESG) is facing some backlash this year as ESG funds fail to produce results similar to their peers. A group of American Airlines employees filed suit against the airline and its investment advisors, alleging that:

> Defendants have breached their ERISA fiduciary duties by investing millions of dollars of American Airlines employees' retirement savings with investment managers and investment funds that pursue leftist political agendas through ESG strategies, proxy voting and shareholder activism—activities which fail to satisfy these fiduciaries' statutory duties to maximize financial benefits in the sole interest of the plan participants.

The plan at issue is $26B with over 100,000 participants. We will be watching this case closely as it questions ESG investments and prudent investing practices using ERISA. *Spence v. American Airlines Inc., Case No 4:23-cv-00552 (N.D. Tex 2023).*

We will also be closely watching new cybersecurity proposals from the SEC regarding when firms must notify customers of breaches and regarding cybersecurity risk management. The rules will impact nearly every entity the SEC regulates, including investment advisers and funds, broker-dealers, clearing agencies, major security-based swap participants, the municipal securities rulemaking board, national securities associations, national securities exchanges, security-based swap data repositories, security-based swap dealers and transfer agents. The SEC received a range of feedback on its cybersecurity proposals at the close of their comment period, ranging from criticism that they are too prescriptive and need further change to support for the rules and calls for tougher provisions.

Cyber

In mid-June 2023, it was discovered that MOVEit, a well-known and popular secure file transfer system app, had been compromised over the Memorial Day weekend. Evidence suggests that the Russian-based group "Cl0p" had discovered a systems vulnerability back in 2021 and had been secretly probing it for almost two years before executing the attack.

Cl0p was able to exploit the vulnerability to download data from the app, including the exfiltration of personal identifiable information. Since then, numerous organizations directly impacted by the attack have received ransom demands. The bad actors have demanded their victims either pay the ransom or risk having Cl0p publish the data, thus exposing the company for not taking enough care to protect sensitive information. Large companies affected by the incident include Shell Oil, Norton LifeLock, Ernst and Young, British Airways and Aer Lingus. That said, there does not appear to be a pattern of who has been victimized by the attack; if a company used MOVEit (or retained a vendor who used the program), then that sensitive information is vulnerable. Cyber insurance policies may provide coverage for costs incurred in conducting mandatory notifications to affected individuals.

There is a continuing trend that cyber breaches target small businesses. In fact, 46% of breaches affected companies with fewer than 1,000 employees. There are a few reasons for this. First, threat actors realize that unlike larger companies, small businesses are more likely to have little to no security protections, making them easier targets. They have also found that they can make the same amount of money by striking larger numbers of small businesses. Attacks on small companies are unlikely to garner media attention. And small companies often fail to alert law enforcement, which lessens the possibility the threat actor will be caught.

Unfortunately, smaller businesses are less likely to maintain cyber coverage and less likely to sustain the expenses arising from a significant breach or extortion event. Sadly, many firms will simply go out of business.

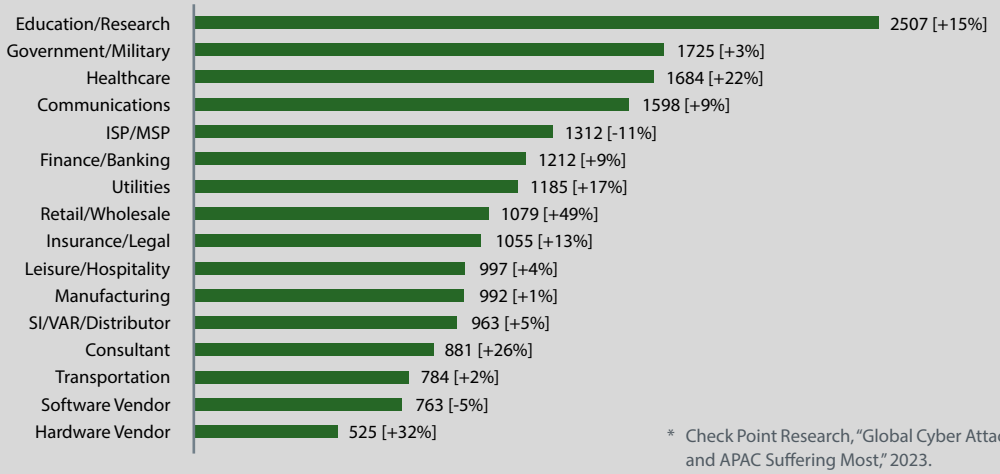
Multifactor authentication (MFA), is generally considered by cyber security experts to be a critical method of protection for businesses. Most cyber insurers refuse to write policies for business clients who fail to confirm they have MFA implemented.

We are now seeing an increase in attackers who are targeting and, in some cases, able to circumvent MFA. One method is to inundate the user with requests for authorization until fatigue sets in and the user approves the request simply to stop the barrage of codes. There are also instances where authentication codes sent by text are intercepted or the user is tricked into providing them via a social engineering scam. Companies should emphasize to their employees the importance of notifying IT security when they receive any suspicious and/or unsolicited messages.

Using an authenticator app loaded onto the user's cellphone is recommended as an additional layer of protection. Such an app provides a constantly changing set of PINs that the user inputs before access is granted.

Cyber Claims on the Rise in 2023[1]

Global Average Weekly Cyber Attacks Per Industry
(2022 Q1 Compared to 2023 Q1)



* Check Point Research, "Global Cyber Attacks Continue to Rise with Africa and APAC Suffering Most," 2023.

Directors and Officers

ESG at the Forefront of Corporate Litigation in 2023

Environmental, social and governance (ESG) has been a hot topic in the financial and business sectors in 2023. Companies have had to answer for pursuing such endeavors or been called to task for not properly executing them.

A California federal court held that a California statute requiring California-based corporations to have a minimum number of directors from designated under-represented groups violates the US Constitution's equal protection clause *(Alliance for Fair Board Recruitment, Plaintiff, v. Shirley N. Weber, in her official capacity as Secretary of State of the State of California, 2:21-cv-01951-JAM-AC (E.D. Cal. May. 16, 2023))*. The California Assembly Bill 979, signed into law in 2020, required public companies headquartered in California to have a minimum number of directors from designated groups that the legislature viewed as historically under represented. The number of directors required depended on the size of the corporation. Legislative and rule-based efforts to diversify corporate boards are not the only initiatives in that area. Internal and external pressures from shareholders, proxy advisors, investment banks, and other organizations and stakeholders have also sought to achieve that goal. Some institutional investors have pushed for board diversity, and some financial organizations have expressed reluctance to finance corporations that do not have sufficiently diverse boards. In addition, legal and business academics have noted the importance of board diversity as a way to improve corporate governance.

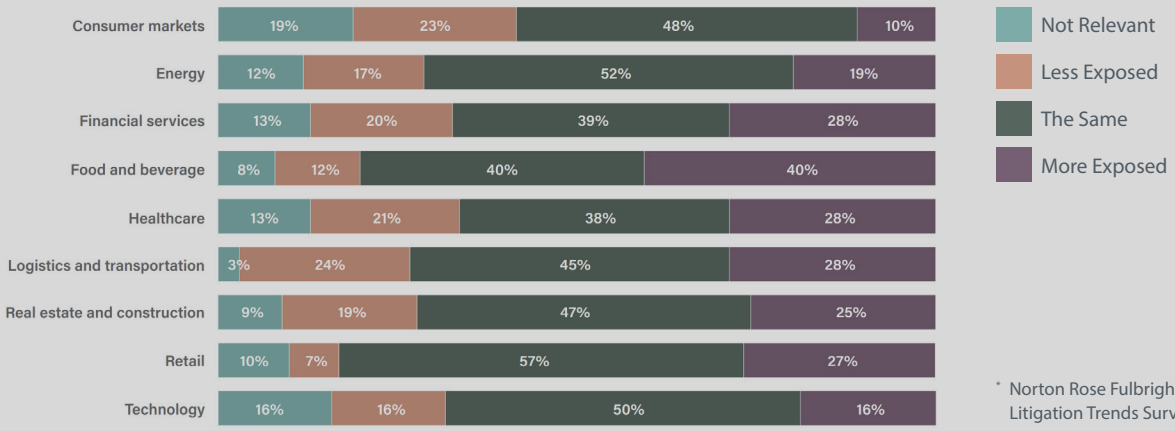
The California decision, which has since been appealed, is one of the latest developments arising from ESG-related endeavors, and despite the resistance the efforts have faced, we expect attention on board diversity will continue.

Over the past couple of years we have also seen businesses publicly tout that they were making progress on ESG goals. Recently, however, there has been a backlash against those that advance ESG. There have been a number of challenges to ESG requirements and endeavors, which have led companies to lower the volume on their ESG initiatives. This is now known as "greenhushing."

Companies are concerned about trying to stay out of the ESG spotlight to avoid the publicity and scrutiny that may follow. This year, two major airlines were hit with ESG backlash lawsuits. In June 2023, an American Airlines pilot filed an ERISA class action *(Bryan Spence, et al v. American Airlines, Inc., et al, No. 4:2023cv00552 (N.D. Tex filed 6/2/2023))*. The lawsuit asserts that the defendants breached their fiduciary duties in violation of ERISA by investing millions of dollars of American Airlines employees' retirement savings with investment managers and investment funds that pursue leftist political agendas through ESG strategies, proxy voting and shareholder activism—activities which fail to satisfy the fiduciaries' statutory duties to maximize financial benefits in the sole interest of the plan participants.

Delta Airlines was hit with a purported class action lawsuit by a California resident who asserted that its claims of carbon neutrality are false and misleading. The suit is what's known as a "greenwashing" lawsuit *(Mayanna Berrin, et al v. Delta Air Lines Inc., No. 2:2023cv04150 (N.D. CA filed 5/30/2023)*.

Change in ESG Dispute Exposure Over the Next 12 Months[1]



* Norton Rose Fulbright. 2023 Annual Litigation Trends Survey

Employment Practices Liability

The first half of 2023 saw continued expansion of pay equality, with the ongoing focus on pay transparency laws. Pay transparency laws have gained popularity over the last two years, beginning with Colorado's Equal Pay Act in 2019.[1] Since then, a number of other states and cities have enacted similar iterations of Colorado's act. California, Washington and Rhode Island all had laws that went into effect on January 1, 2023, with New York's law going into effect in September 2023. The common theme is that employers are now required to list salary ranges on job postings and/or provide pay ranges to job applicants upon request. This will likely be a continuing trend for the second half of 2023. The map below shows which states have passed a version of pay transparency protections.[2]

Artificial intelligence (AI) is an ongoing hot topic, especially in the wake of generative AI systems such as ChatGPT, a natural-language processing tool that uses AI technology to allow users to have human-like conversations with the chatbot. Since its launch, it has become one of the fastest-growing phenomena in modern technological advancements, and the chatbot's use is becoming more widespread. Among people at work, 41% said they use the AI site to generate ideas and 20% use it to create content.[3] Its growth has sparked debates regarding the appropriate use in the business context and potential legal implications.

In the same vein, there is an increased awareness of the use of AI in human resources decision-making and the potential for discrimination and harassment, prompting the Equal Employment Opportunity Commission to release a technical guide, Assessing Adverse Impact on Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures Under Title VII of the Civil Rights Act of 1964.[4]

States are leading the legal charge on the equal pay front. We are tracking the states that have pending legislation that would enhance equal pay protections in the state. We have also categorized the existing laws to help employers navigate their equal pay obligations. New York and California have recently enacted significant overhauls to equal pay legislation markedly increasing statutory protections. Seven states have incorporated some elements of major equal pay protections, such as statutorily changing what constitutes a "comparator group" or weakening employers defenses. Finally, twenty-seven states have enacted legislation with minor modifications to existing equal pay protections.

The Sixth Circuit Court of Appeals adopted a new standard required for a district court to facilitate notice of a Fair Labor Standards Act (FLSA) collective action to employees who were not originally parties to a suit. In Brooke Clark, et al v. A&L Homecare and Training Center, LLC, et al, the court rejected two long-standing approaches, Lusardi and Swales, and imposed a tougher standard: the preliminary injunction standard. The Sixth Circuit held that "for a district court to facilitate notice of an FLSA suit to other employees, the plaintiffs must show a 'strong likelihood' that those employees are similarly situated to the plaintiffs themselves."

In the wake of the Dobbs decision, there has been an uptick in legislation regarding reproductive health, including coverage for abortions, contraceptives and infertility treatment.

California, New York and Rhode Island have expanded leave requirements, including paid family and bereavement leave.

Policies against hair discrimination are receiving federal support. On March 18, 2023, the House passed the Creating a Respectful and Open World for Natural Hair Act (or CROWN Act) which protects individuals from discrimination over natural and protective hairstyles. The bill is currently before the Senate. To date, 22 states have signed the CROWN Act.[5]

Below is a map of the states that have passed the CROWN Act to date. [6]

[1] Equal Pay For Equal Work Act | Colorado General Assembly

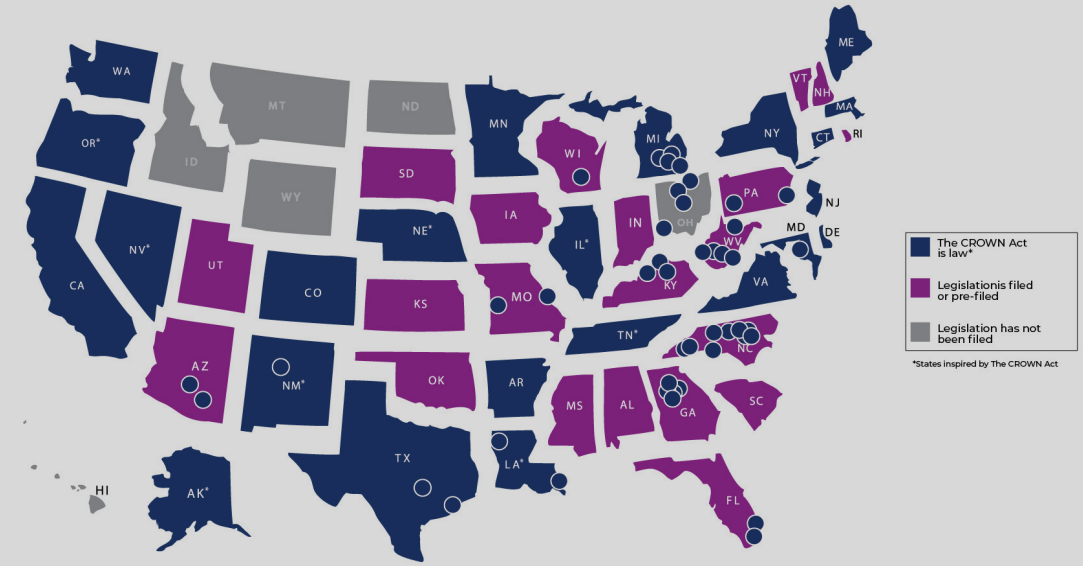
[2] Updated Maps: States With Equal Pay Protections and Pending Equal Pay Legislation | Equal Pay Pulse (orrick.com)

[3] How ChatGPT Is Catching On in America | WordFinder® (yourdictionary.com)

[4] Select Issues: Assessing Adverse Impact in Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures Under Title VII of the Civil Rights Act of 1964 | U.S. Equal Employment Opportunity Commission (eeoc.gov)

[5] About — The Official CROWN Act (thecrownact.com)

[6] Ibid



THE CROWN ACT IS LAW

Beckley, WV	Philadelphia, PA	Wauwatosa, WI	Durham, NC	Tempe, AZ	Austin, TX
Charleston, WV	Pittsburgh, PA	Covington, KY	Orange County, NC	Tucson, AZ	Dallas County, TX
Huntington, WV	Newburgh Heights, OH	Frankfort, KY	Greensboro, NC	Clayton County, GA	Harris County, TX
Lewisburg, WV	Akron, OH	Lexington, KY	Raleigh, NC	East Point, GA	Pflugerville, TX
Morgantown, WV	Columbus, OH	Louisville, KY	Winston-Salem, NC	Gwinnet County, GA	Shreveport, LA
Wheeling, WV	Cincinnati, OH	Ashville, NC	Albuquerque, NM	South Fulton, GA	New Orleans, LA
Ann Arbor, MI	Newburgh Heights, OH	Buncombe County, NC	Kansas City, MO	Stockbridge, GA	
Ingham County, MI	Dane County, WI	Chatham County, NC	St. Louis, MO	Broward County, FL	U.S. Virgin Islands
Genesee County, MI	Milwaukee, WI	Charlotte, NC	Montgomery County, MD	Miami Beach, FL	

Significant Coverage Litigation Decisions

According to the Rhode Island Supreme Court, context matters when reviewing policy language to determine coverage, especially policy exclusions *(Regan Heating & Air Conditioning v. Arbella Protection Insurance Co., No. 2020-170-Appeal)*. In the case at issue, the insured accidentally caused 170 gallons of home heating oil to leak into its customer's basement, resulting in property damage. The insurance company denied the claim based on a pollution exclusion, and the insured sued for coverage.

> In ruling in **favor** of the insured, the **court found** that while a substance such as heating oil **might be considered** a **pollutant** in one context, the fact that it is involved in a loss **does not** make it pollution.

The court determined that the insured could reasonably expect that such a loss as oil spilling into a customer's basement would be covered under its policy. Conversely, heating oil spilling into the ground would more likely be considered pollution. Ultimately, the context mattered.

In *BrightView Enterprise Solutions, LLC v. Farm Family Casualty Insurance Company, No. 20cv7915 (EP) (AME), 2023 U.S. Dist. LEXIS 20764 (D.N.J. Feb. 7, 2023)*, the court ruled an insurance company's decision not to settle was unreasonable, and they may still be liable for bad faith even if the policyholder prevails at trial. The litigation involved three entities, all insured under the same policy. An employee of the company they were performing work for was injured and sued the three companies. The insurer initially agreed to defend and provide coverage for all three defendants up to its $1M policy limit.

Prior to trial, the insurer offered only a fraction of the amount that was communicated to the policyholders and insurer on what it would take to settle the matter. Two of the insureds, after demanding the insurer settle the matter within policy limits, wound up settling out of court and reserved rights to seek recovery from the insurer. The remaining policyholder was successful at trial in defeating the claim. Afterwards, the additional insureds filed a lawsuit against the insurer, asserting a bad faith breach of contract claim and seeking to recoup the settlement payment, among other damages. The insurer moved for summary judgment, arguing that there was no genuine dispute of material fact that they negotiated in good faith. The court disagreed, finding that the insurer's evaluation and negotiations were cursory and conducted without taking into account all the information at hand and, as such, those negotiations were in bad faith.

The Seventh Circuit upheld a lower court ruling that an insurance company was obligated to defend its insured against allegations that it violated the Illinois Biometric Information Privacy Act (BIPA), finding that the policy's broad catchall coverage exclusion provision is too ambiguous to be enforceable *(Citizens Insurance Co. of America v. Wynndalco Enterprises LLC et al., case number 22-2313, in the U.S. Court of Appeals for the Seventh Circuit)*.

The plaintiffs alleged the insured served as a vendor for artificial intelligence company Clearview AI to sell its database of more than 3 billion facial scans collected from social media in violation of BIPA. The insurance company denied coverage, relying on an exclusion in the policy that precluded coverage for violations of the Telephone Consumer Protection Act, the CAN-SPAM Act, the Fair Credit Reporting Act, and the Fair and Accurate Credit Transaction Act. They also relied on a catchall provision in the policy that read "any other laws, statutes, ordinances, or regulations, that address, prohibit or limit the printing, dissemination, disposal, collecting, recording, sending, transmitting, communicating or distribution of material or information."

The Seventh Circuit agreed with the lower court that, on its face, the catchall provision is "intractably ambiguous." The court further rejected the argument that the language encompassed statutes like BIPA, stating that it did not find that the aim of the exclusion was to not cover privacy claims.

A federal court rejected an insurance company's late notice defense, despite the policyholder's admissions the claim notice was not timely, because the insurance company failed to explicitly deny coverage on that ground *(Mave Hotel Investors LLC v. Certain Underwriters at Lloyd's London No. 21-cv-08743 (JSR), 2023 U.S. Dist. LEXIS 62718 (S.D.N.Y. Apr. 10, 2023))*.

The dispute arose from a claim under a property policy for damage to hotel rooms. The insurer issued its final coverage position, denying coverage based on a wear-and-tear exclusion. Within the letter there was a general reservation of rights under the policy and at law to raise additional defenses as bars to coverage. In the subsequent coverage litigation that followed, the insurer filed a motion for summary judgment and included an argument that there should be coverage due to late notice. Countering their argument, the policyholder argued that the insurer had waived its right to raise late notice as a defense, as they had not cited such in their declination letter.

The court agreed that the insurer had waived its late notice defense by denying coverage on the basis of wear-and-tear but not late-notice. The court reasoned that at the time the final declination letter had been issued, the insurer had all the information they would have needed to be able to raise the notice issue and failed to do so.

Meet the Specialists

Contacts

Contacts

Lauren Kim
Managing Director
Financial Institutions Group
Phone: 224.649.5223
Email: lauren.kim@nfp.com

Jon Franznick
Senior Vice President
Head of Claims Advocacy
Phone: 212.301.1096
Email: jonathan.franznick@nfp.com

Moire Moron
Vice President
Management & Prof. Liability, Claims Advocacy
Phone: 404.504.3819
Email: moire.moron@nfp.com

Chris Krako
Vice President
Management & Professional Liability
Claims Advocacy
Phone: 516.327.2819
Email: chris.krako@nfp.com

Matthew Plotkin
Assistant Vice President
Management & Professional Liability
Claims Advocacy
Phone: 516.327.2848
Email: matthew.plotkin@nfp.com