Legal Matters®

Business Law
spring 2022

Business advocates seek further extension of COVID liability shields

Business groups are arguing for the continuation of COVID-19 liability shield laws that are about to expire.

Thirty states enacted these measures in 2020 and 2021. The laws provide expansive immunity for businesses and other entities from lawsuits claiming liability for an individual's exposure, injury or death due to COVID-19.

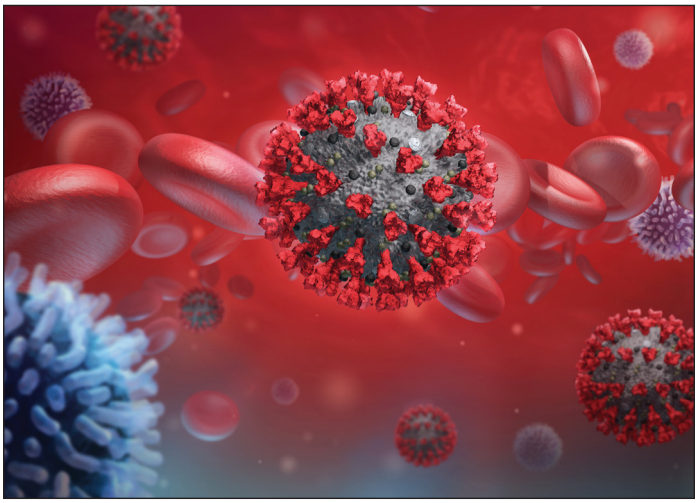
Under most of these measures, a plaintiff can only sue a business if they can show reckless conduct, gross negligence, or something similar.

In certain states, the liability shield laws include provisional liability limits that are set to expire soon. In other states, they already have expired, such as in Ohio, where the shield ended at the end of September.

While GOP pressure is mounting to extend these protections for businesses, many legislatures are not as focused on legislation related to COVID at this point.

COVID-19 liability protections are scheduled to end in several states in 2022, including Alabama, Georgia, Idaho, Kansas, South Dakota, and Tennessee. Limits are scheduled to continue into 2023 in some states, such as Arkansas and Kentucky.

Plans to renew the shields are on the radar in Georgia, which has a relevant law set to expire in July. The law was passed in 2020 and was extended for another year in 2021.



©alphaspirit

Labor unions contend that pandemic-related liability shields could lead businesses to reduce the precautions they take to protect workers and customers from COVID-19.

But business groups claim that the shields are needed to protect companies from litigation that could damage businesses or even cause smaller ones to shut down.

In 2020, when the pandemic began, a proposed liability shield

continued on page 3

MAHDAVI BACON HALFHILL & YOUNG, PLLC

11350 Random Hills Road, Suite 700 | Fairfax, VA 22030
(703) 352-1300 | admin@mbhylaw.com | www.mbhylaw.com

‘Greenwashing’ raises cybersecurity risks

© Faithie

Organizations that make environmental, social and governance (ESG) claims had better be able back them up or risk attacks from “hacktivists.”

Research from the University of Delaware suggests companies that engage in “greenwashing” or otherwise fake corporate social responsibility efforts are at higher risk for cybersecurity attacks.

John D’Arcy, who led the research, said there is emerging evidence that at least some members of the hacking community are motivated by a cause, rather than financial gain.

D’Arcy and his coauthors used a unique dataset that included information on data breaches as well as an external assessment of firms’ ESG performance.

The study found that firms that engage in marketing or other peripheral efforts meant to give the appearance of corporate social responsibility without embedding those causes within the fabric of their operations are more likely to experience hacking events.

According to the study, these issue-motivated hackers may include disgruntled employees as well as external hacktivist groups looking to punish poor actors and influence corporate change.

Conversely, according to the study, firms that engage in more meaningful forms of corporate social responsibility experienced fewer hacks and data breaches.

Companies should be careful about promoting social actions without sufficient evidence to show those efforts are authentically motivated and part of larger systemic efforts throughout their core business practices.

We welcome your referrals.

We value all of our clients. While we are a busy firm, we welcome your referrals. We promise to provide first-class service to anyone that you refer to our firm. If you have already referred clients to our firm, thank you!

‘No poach’ agreements under scrutiny

The Department of Justice (DOJ) is targeting “no poach” and “no hire” agreements. The shift could have a lasting effect on how companies recruit and retain workers.

In 2010, the DOJ brought civil charges against a number of Silicon Valley companies that were alleged to have a secret pact not to poach each other’s employees. In a civil settlement, Adobe, Apple, Google, Intel, and Intuit agreed to abandon their no poach practices.

By 2016, after additional years of investigation and enforcement, the DOJ warned that no poach activities could warrant criminal penalties.

Finally, in January of last year, the DOJ made good on its threat when a federal grand jury indicted Surgical Care Affiliates LLC for agreeing with competitors not to solicit each other’s senior-level team members.

A second company was indicted in March 2021 after a manager allegedly agreed not to recruit nurses from a competitor. In December, a jury reached another no-poach indictment, this time in the aerospace industry.

Meanwhile, several state attorneys general have been targeting similar violations. Previously, state actions have compelled fast food chains to eliminate no poach provisions from their franchise agreements.

Recently, in September 2021, Old Republic National Title Insurance Co. agreed to pay $1 million in penalties after a New York state probe into no-poach activities.

Meanwhile, the Biden administration is reviewing the Federal Trade Commission’s (FTC) authority to curtail the use of non-competes and other clauses that limit workforce mobility. The DOJ and FTC held a joint workshop in December which, reportedly, placed some emphasis on issues of non-competes and no poach agreements.

©AndreyPopov

Businesses should note that no poach agreements don’t just occur at the executive level. Managers and other mid-level leaders may be equally responsible, considering these informal agreements the polite way to do business with their peers in the industry. Businesses are advised to educate leaders at all levels, making sure team members are aware of competition law and growing federal scrutiny.

Talent analysts say enforcement is expected to be an area of focus throughout the Biden administration.

Allowed OSHA violation leads to fine

In a case where a foreman allowed a member of his crew to continue working in the wake of an Occupational Safety and Health Administration (OSHA) rules violation that had not been fixed, a $35,000 penalty against the company must stand, according to a decision issued by a federal appellate court.

The case, which took place in Texas, is a warning for businesses to ensure workers' strict compliance with OSHA rules and fix any violations promptly.

A safety manager who worked for the construction company had clearly told the foreman to fix the violation.

The company argued that the foreman's failure to fix it while allowing his crew to continue working constituted "unpreventable employee misconduct." Further, it claimed that the OSHA violation was not "willful" because the manager specifically instructed the foreman to fix the violation.

Under the "unpreventable employee misconduct" defense, even if OSHA makes a case for unlawful conduct, a company is not liable if it can demonstrate that the violation resulted from unpreventable employee misconduct. But the defense is only valid if the company can prove that it both has and enforces relevant safety standards.

©AndreyPopov

In the Texas case, the court said that although the company had safety rules in place, it failed to properly enforce them. Therefore, it said, the defense could not be used.

The company also failed to discipline the foreman for the violation and didn't impose discipline for at least one other prior violation. The court took this data to mean that the company didn't enforce its safety rules.

The court also said that the foreman's failure to follow the safety manager's instruction was an indication of a willful violation.

Biden administration expands availability of seasonal visas

It's no secret that there is an ongoing labor shortage, spurred by the COVID-19 pandemic. In response, the Department of Homeland Security (DHS) and the Department of Labor (DOL) announced that they will make available an additional 20,000 H-2B temporary nonagricultural worker visas.

The new influx of visas allows for a total of more than 50,000 seasonal visas this year.

The H-2B visa program allows companies who meet specific regulatory requirements to bring in foreign nationals to take on temporary nonagricultural positions.

Typically, companies in seasonal industries, such as hotels and ski resorts, rely on the program.

With this type of visa, workers must be hired for a limited period of time. Businesses are required to certify that there is an insufficient pool of U.S. workers to fill the job and that their use of the visa program will not have a negative effect on wages for U.S. workers in similar roles.

While the increase in visas might be of some help, the number of visas is still small in comparison to the number of open jobs. Also, be aware that applying for H-2B visas can be costly for companies.

Business advocates seek further extension of COVID liability shields

continued from page 1

that would have applied nationwide didn't make it through Congress.

Generally, amidst the lawsuits that have been filed related to COVID-19, a relatively small percentage has reportedly involved the sort of personal injury claims the liability shields are meant to block. For one thing, in most cases, state workers' comp laws bar injury claims by workers involving illness or injury at work.

However, a California appeals court decided that a factory worker whose husband died of COVID-19 could sue her employer, claiming that his death resulted from her exposure at work. The company argued that the case should fall under the workers' comp system.

MAHDAVI
BACON
HALFHILL &
YOUNG, PLLC
ATTORNEYS AT LAW

11350 Random Hills Road, Suite 700 | Fairfax, VA 22030
(703) 352-1300 | admin@mbhylaw.com | www.mbhylaw.com

LegalMatters | spring 2022

FTC prioritizes fighting COVID-related scams


©Gajus-Images

The Federal Trade Commission says that fighting fraud scams in the wake of the COVID-19 pandemic remains "a top priority for the Commission, and we will use every weapon in our arsenal to do so."

The comments were made in testimony in front of the U.S. Senate Commerce Committee's Subcommittee on Consumer Protection, Product Safety, and Data Security.

The FTC testified that it is focused on finding and addressing COVID-related fraud that affects both businesses and consumers and working on identifying related trends.

Various scams are happening that prey on businesses in the midst of the upheaval resulting both directly and indirectly from COVID-19.

They include such things as fake messages sent to employees that appear to come from the CEO or boss asking workers to transfer funds to them, fake phone calls from technology staff members asking for company passwords, and messages that appear to come from the Centers for Disease Control and Prevention (CDC) asking for personal information.

With a significant rise in the number of businesses that are operating online, the FTC said that it has seen a surge in reports related to undelivered merchandise, losses from online shopping and business imposters. The Commission said complaints about cryptocurrency investment scams and other income scams have been proliferating, in addition to complaints about medical treatments.

The testimony noted the FTC's use of the Consumer Sentinel Network, an investigative cyber tool that provides access to reports on consumer complaints about fraud and other matters.

Complaints have led to "numerous" law enforcement actions and prosecutions under the federal COVID-19 Consumer Protection Act, the FTC said. That law grants the FTC the authority to seek civil penalties from individuals who commit fraud.

The FTC cited enforcement actions it has taken relevant to false health claims and fraud that preyed on the financial distress of small business owners.

The FTC "will remain vigilant in protecting the public from harms that stem directly and indirectly from the COVID-19 pandemic," the agency said in the testimony.