Ridgemark Insurance Services

JANUARY 2022 | VOLUME 3 | ISSUE 1

NEWSALERT

Business and Economy

Stay on Top of New Laws, Rules in New Year

EVERY YEAR starts with a flurry of new laws and regulations that California employers have to contend with.

And 2022 is no different as the California legislature had a busy year and the stresses of the COVID-19 pandemic resulted in more activity. The end result is another round of new laws that employers need to stay on top of so they don't run afoul of them.

With no further ado, here are the top regulations and laws affecting California businesses.

1. Big change to Cal/OSHA citations

SB 606 adds two new Cal/OSHA violation categories for purposes of citations and abatement orders: "enterprise-wide" and "egregious" violations. Cal/OSHA can issue an enterprise-wide citation that would require abating the violation at all locations. And the employer can face a maximum penalty of $124,709 per violation.

The law also authorizes the agency to issue a citation for an egregious violation if it believes that an employer has "willfully and egregiously" violated a standard or order. Each instance of employee exposure to that violation will be considered a separate violation and fined accordingly.

2. Permanent COVID standard

On Sept. 17, 2021, Cal/OSHA released a draft text for proposed permanent COVID-19 regulations, which if adopted would be subject to renewal or expiration after two years and would replace the current emergency temporary standard, which is set to expire Jan. 14, 2022.

Adoption is expected in the spring of 2022. Here's some of what the draft standard would do:

CDPH rules – It would require that employers follow California Department of Public Health COVID-19 prevention orders.

Masks for unvaxxed staff – Unvaccinated staff must wear masks. Employers must provide masks when the CDPH requires them.

Outbreak rules – During an outbreak in the workplace, all staff would be required to wear face coverings regardless of vaccination status. Employers would need to provide respirators during major outbreaks to all employees.

3. COVID exposure notification

On Oct. 5, 2021, AB 654 took effect, updating requirements for what an employer must do if there is an outbreak of COVID-19 cases at its worksites.

This law somewhat curtailed earlier outbreak-reporting requirements as well as other required notifications for certain employers, and updated several provisions of the 2020 outbreak notification law, AB 685.

Here are some highlights:

- Employers have one business day or 48 hours, whichever is later, to report a workplace COVID-19 outbreak to Cal/OSHA and local health authorities.
- Employers do not need to issue these notices on weekends and holidays.
- When an employer has multiple worksites, it only needs to notify employees who work at the same worksite as an employee who tests positive for coronavirus.
- The new definition of "worksites" for the purposes of the law has been changed to exclude telework.

See 'Workers' on page 2

Ridgemark Insurance Services Wishes You a Happy New Year

Ridgemark Insurance Services

Ridgemark Insurance Services

2130 Professional Drive, Ste 225,
Roseville, CA 95661

Phone: 916-306-1550
www.ridgemarkinsurance.com

If you would like to receive this newsletter electronically, e-mail us at:
info@ridgemarkinsurance.com

Continued from page 1

Workers Can Take Family Medical Leave to Care for In-Laws

4. Expansion of the California Family Rights Act

AB 1033 expands the CFRA to allow employees to take family and medical leave to care for a parent-in-law with a serious health condition.

More importantly, it adds a requirement that mediation is a prerequisite if a small employer (one with between five and 19 workers) is the subject of a civil complaint filed by one of its employees.

5. Workplace settlement agreements and NDCs

A new law took effect Jan. 1 that bars employers from requiring non-disclosure clauses in settlement agreements involving workplace harassment or discrimination claims of all types. This builds on prior law that barred NDCs only in cases of sex discrimination or sexual harassment.

The new law expands that prohibition to all protected classes, such as: race, religion, disability, gender, age, and more.

One important note: While employees can't be prohibited from discussing the facts of the case, employers can still use clauses that prohibit the disclosure of the amount paid to settle a claim.

6. OSHA vaccine mandate

As of this writing, Fed-OSHA's new emergency COVID-19 standard was set to take effect on Jan. 1, with the most contentious part of the rule mandating that employees who work for employers with 100 or more staff be vaccinated or submit to weekly testing.

Unvaccinated workers would also be required to wear masks while on the job under the new rules, which have faced fierce challenges in courts.

The U.S. Court of Appeals for the Sixth District recently reversed a stay of the order as challenges to it are litigated, meaning the order can take effect as scheduled as the legal process challenging the rule proceeds.

The U.S. Supreme Court will hear expedited arguments Jan. 8 on the U.S. Court of Appeals for the Sixth Circuit's decision to lift the Fifth Circuit's stay.

7. Wage theft penalties

AB 1003, which took effect Jan. 1, added a new penalty to the California Penal Code: Grand Theft of Wages. The new law makes an employer's intentional theft of wages (including tips) of more than $950 from one employee, or $2,350 for two or more workers, punishable as grand theft.

The law, which also applies to wage theft from independent contractors, allows for recovery of wages through a civil action.

As a result, employers (and potentially managers and business owners) would be exposed to both criminal and civil liability for wage and hour violations like failing to pay staff accurately and in a timely manner.

Review your compensation policies and practices to make sure you are in compliance with current wage and hour laws.

8. COVID cases may be included in X-Mods

The Workers' Compensation Insurance Rating Bureau of California has proposed plans to start requiring COVID-19 claims to be included when calculating employers' X-Mods.

The proposal, which would have to be approved by the state insurance commissioner, would bring to an end current rules that exclude the impact of COVID-19 workers' compensation claims on X-Mods.

If approved, the new rule would take effect on Sept. 1, 2022. That means that employers will be held accountable for COVID-19-related workers' compensation claims and, if any employee needs treatment or dies from the coronavirus, it could result in higher premiums in the future.

9. Notices can be e-mailed

A new state law authorizes employers to distribute required posters and notices to employees via e-mail. SB 657 adds e-mail as a delivery option to the list of acceptable notification methods, which also includes mail.

Required posters and notices will still need to be physically posted in the workplace.

10. Warehouse quota rules

A new law that took effect Jan. 1 makes California the first (and only) state to regulate quotas used by warehouse employers.

While the bill was written with Amazon Inc. in mind, it affects all warehouses with 100 or more workers, and violations of the new law can be costly for an employer.

Under AB 701, warehouse employees must be provided with a written description of the quotas to which they are subject within 30 days of hire. Common quotas include the number of tasks the employee is required to perform, the materials to be produced or handled, and any adverse employment action that may result from a failure to meet the quota.

While employers may still implement quotas, employees are not required to meet a quota if it:

- Prevents them from taking required meal or rest periods,
- Prevents them from using the bathroom (including the time it takes to walk to and from the toilet), or
- Contravenes occupational health and safety laws.

The law also bars employers from discriminating, retaliating or taking other adverse action against an employee who:

- Initiates a request for information about a quota or personal work-speed data, or
- Files a complaint alleging a quota violated the Labor Code. ❖

Software Security Hole Puts Firms at Risk

THE FEDERAL government is warning that a newly discovered computer software vulnerability poses a major threat to the security of computer networks around the country.

Cyber criminals are exploiting holes in open-source code software commonly used in computer applications, websites and cloud services, which can allow them to seize control of a business's computer network if preventative measures are not taken.

This is not a threat that businesses should take lightly as it could cripple your organization if your network is affected. If your firm is large enough to have dedicated IT staff, it should be their focus now.

The danger

The vulnerability lies in the Log4j software library, written in the Java programming language and created by the Apache Software Foundation.

Many software vendors incorporate the Log4j software library into products such as websites, applications and cloud services to record network security and performance information.

It is likely that some of the software your business uses is built around Log4j. It runs on everything from cloud services to business enterprise software to internet-connected devices such as security cameras.

The federal Department of Homeland Security, the National Security Agency and other agencies announced on December 10 that they were "responding to active, widespread exploitation" of the vulnerability.

They warned that, if a company's software has this vulnerability, a criminal could take over the network and cripple the business.

What you should do

Do not take this threat lightly. As stated above, if you have dedicated IT staff, make it their primary focus right now.

Major software developers have reported that their products have the vulnerability.

Vulnerable Brands

Software developed by these firms have the security hole:

- Microsoft
- McAfee
- Hewlett Packard
- IBM
- Red Hat
- Dell
- Cisco
- Adobe
- Salesforce
- Oracle

You can find the full list of affected vendors and software here.

Apache has published three software patches to address the problem since it became known. Software developers who use Log4j are likely applying the patches and making updates to their software available to business users.

If you receive notification about an updated version of software you are using, it should be installed promptly.

Companies that do not have their own IT department, should contact computer network consultants as soon as possible to get advice on how to proceed.

The Cybersecurity & Infrastructure Security Agency has technical information on this threat on a dedicated website. IT experts should review the site's content, take appropriate actions as soon as possible, and monitor the site for further updates to the situation.

In the meantime, system administrators should adjust logging system settings so it does not interpret data as computer code.

Antivirus software, using a virtual private network for remote access to the system, and being alert for phishing e-mails are also important protections. Sound network data security coupled with safe internet practices can protect your business's systems and your ability to continue operating. ❖

Protecting Against Workplace Sexual Harassment

BY NOW, ALL employers should realize and understand that sexual harassment is illegal. Employers are directly responsible for employee behavior, which gives harassed workers recourse in bringing legal actions against those that employ them.

According to the Equal Employment Opportunity Commission, there were 11,497 sexual harassment complaints in 2020 in the U.S..

Any employer that's ever been involved in a sexual harassment suit can attest that the cost to settle or defend such a lawsuit can be jaw dropping. Defense and settlement can easily run to several hundred thousand to several million dollars, or more.

What constitutes sexual harassment?

State and federal law prohibits superiors from demanding sexual acts in exchange for preferential treatment or under threat of punitive measures. The following are examples of such behavior:

- Altering expectations of job performance when a subordinate repeatedly refuses advances for a date or sexual encounter.
- A superior demanding sexual acts in order for a subordinate to receive a raise or promotion.
- Disciplinary action, including termination, of a subordinate who refuses sexual advances or ends an existing romantic relationship.

However, sexual harassment doesn't always involve a subordinate/authority figure relationship. An offender can be anyone from a co-worker to a customer or business vendor.

The offender can be male or female, as can the victim. Furthermore, the victim doesn't even need to be the employee actually harassed.

Anyone that's affected by the harassing or offensive behavior can be termed a victim.

Verbal, visual, physical or written ... any behavior that causes another employee to view the work environment as hostile, or is unwanted or focuses on the sexuality or gender of another person, may constitute sexual harassment.

Specific examples of such would be teasing, suggestive objects or pictures being displayed, and repetitively requesting sexual acts or dates.

Employment practices liability insurance

Businesses can financially protect themselves with employment practices liability insurance.

While policies vary, EPLI generally covers settlement, judgment and incurred legal costs arising from an array of incidents:

- Wrongful termination,
- Employment contract breaches,
- Employment and promotion failures,
- Wrongful disciplinary actions,
- Wrongful emotional distress infliction,
- Negligent employee evaluations, and
- Discrimination.

Some policies automatically include sexual harassment as well, but others may not. Or you may be required to get a special endorsement for sexual harassment.

Coverage is specific. Before purchasing a policy, decide who should be covered. For example, should full- and part-time employees, contracted persons, supervisors, department heads, subsidiaries, company divisions, and so forth be covered or not?

One other note about EPLI is that it's mandatory for employers to report incidents within a reasonable amount of time.

Keep in mind that EPLI cost is based on the business type, employee numbers and past lawsuits associated with the organization.

Preventing sexual harassment

Prevention is the cornerstone of reducing the risk of a sexual harassment lawsuit.

Finally, if your firm has EPLI, any incident should be reported to your insurer immediately. ❖

Put Policies in Place

- Create, communicate and enforce a zero-tolerance policy for workplace sexual harassment.
- Have an effective harassment complaint process in place and take immediate, consistent and appropriate action when a complaint is made.
- Thoroughly document all complaints and the following investigation and actions.