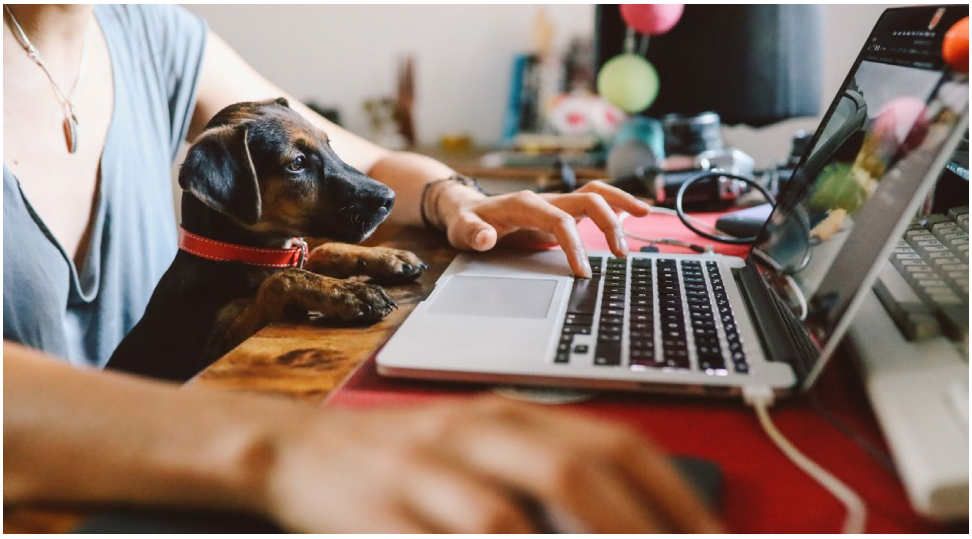
Ridgemark Insurance Services

JULY 2020 | VOLUME 1 | ISSUE 1

NEWSALERT

Workers' Compensation

New Telecommuter Class Code in the Works



DUE TO the COVID-19 pandemic, California's workers' compensation rating agency plans to implement a new class code for telecommuting employees on Jan 1, 2021.

The Workers' Compensation Insurance Rating Bureau of California started work on the new classification as companies ordered employees to start working at home after stay-at-home orders were issued to contain the spread of the coronavirus.

The new code for telecommuting workers will be 8871. Under a prior emergency rule, the Rating Bureau had recommended that employees who were thrust into telecommuting because of the COVID-19 outbreak be assigned the 8810 "Clerical Office Employee" code.

This is a major change in the class code structure and will affect employers throughout the state. If you have telecommuting staff, you should prepare for this change now.

The specifics

Until now, telecommuting employees whose duties meet the definition of clerical employees in the California Workers' Compensation Uniform Statistical Reporting Plan have been assigned class code 8810 "Clerical Office Employees," or their employers' standard classification if that classification specifically includes clerical office staff.

Rating Bureau staff has proposed that class code 8871 be the code for clerical employees who work more than 50% of their time at their home or other office space that is not on the employer's premises.

As mentioned, the class code will be used only if the class code for the employer does not include clerical employees. Currently there are 41 class codes that include clerical staff. There are also two codes that specifically exclude them. If a company includes all of its staff in the same code, any clerical staff on its payroll are not assigned the 8810 "Clerical Employee" class code and instead assigned the code for the company as a whole.

For the sake of continuity, the Rating Bureau staff has recommended that those 43 class codes be amended to specifically include or exclude clerical telecommuting staff.

What you should do

If you have staff on your payroll who are telecommuting, you should start preparing your accounting or bookkeeping software to add in this code for when your policy comes due in 2021.

Starting work on this now can help your insurer more accurately price your future policies, or when they decide to audit your payroll.

Conversely, you should not attempt to change the class code for your currently telecommuting employees now or at any time before Jan. 1, 2021, as the final rules have not yet been written, approved or promulgated. They also need to be approved by the state insurance commissioner.

The Rating Bureau plans to apply the rate for the class code for clerical employees to the new class code for the first few years, and until it can gather enough data to set a unique rate for the code.

That could take a few years as the Rating Bureau typically uses a window of the past three years of claims experience and costs when setting class code rates.❖

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

Cloud Services

Attacks Grow Amid Work-From-Home Boom

AS MORE OF America's workers were asked to work from home due to the COVID-19 pandemic, cyber criminals jumped at the opportunity to take advantage, it seems.

Remote work means work being handled on the cloud as employees share files and need a convenient way to access them.

But cyber criminals are banking on workers letting down their guards when they work from home, so it's no surprise that while cloud service usage among enterprises jumped 50% between January and April, external attacks on cloud accounts boomed 630% in the same period.

Also, hackers and other cyber scammers orchestrated systematic attacks on collaboration tools like Cisco WebEx, Zoom, Microsoft Teams and Slack, according to the "Cloud Adoption & Risk Report – Work from Home Edition" report by McAfee.

The risk to enterprises cannot be overstated as criminals try to take advantage of the sudden shift to telecommuting by thousands and thousands of organizations as they try to cope with the COVID-19 pandemic and continue operating during stay-at-home orders.

Employees are your first line of defense. You can protect your company by encouraging them to be skeptical of e-mail from unfamiliar sources.

Training your staff

The preferred method hackers use to gain access to network and cloud files is through phishing and ransomware attacks.

Consulting firm PricewaterhouseCoopers recommends coaching your staff to take the following precautions, particularly on their mobile devices:

- Be skeptical of e-mails from unknown senders, or from people (like your company's CEO) who do not usually write directly to you.
- Don't click on links or open attachments from those senders.
- Don't forward suspicious e-mails to co-workers.
- Examine the sender's e-mail address to ensure it's from a true account. Hover over the link to expose the associated web addresses in the "to" and "from" fields; look for slight character changes that make e-mail addresses appear visually accurate – a .com domain where it should be .gov, for example.
- Grammatical errors in the e-mail text are a sure sign of fraud.
- Report suspicious e-mails to the IT or security department.
- Install the company-approved anti-phishing filter on browsers and e-mails.
- Use the corporate-approved anti-virus software to scan attachments.
- Never donate to charities via links included in an e-mail; instead, go directly to the charity website to donate.

Cyber insurance

Cyber insurance is designed to protect your company by insuring you for network security issues, privacy, interruption to your business, media liability, and errors and omissions.

For phishing, ransomware and other cyber attacks, the network security and business interruption portion of the policy would mainly come into play.

Network security coverage – This includes first party costs. That is, expenses that you incur directly as a result of a cyber incident, including:

- Legal expenses
- IT forensics
- Negotiation and payment of a ransomware demand
- Data restoration
- Breach notification to consumers
- Setting up a call center
- Public relations expertise
- Credit and identity monitoring
- Restoration.

Business interruption – When your network, or the network of a provider that you rely on to operate, goes down due to an incident, you can recover lost profits, fixed expenses and extra costs incurred during the time your business was impacted. This includes loss arising from:

- Security failures, like a third party hack.
- System failure. ❖

OSHA Asks Employers to Investigate Illness Claims

IN LATE MAY Fed-OSHA issued new guidance asking employers to investigate COVID-19 cases among their workers and report those that they deem were contracted in the workplace.

The guidance recommends employers investigate the genesis of all COVID-19 cases among employees.

Under the guidance, employers must "make reasonable efforts" to investigate confirmed cases in the workplace.

OSHA said it does not expect employers, especially small employers, to undertake extensive medical inquiries, given employee privacy concerns and most employers' lack of expertise in this area.

OSHA said it would usually be sufficient to follow the probe parameters below.

INVESTIGATING A COVID-19 CASE

- Ask the employee how they believe they contracted COVID-19.
- While respecting employee privacy, discuss with them their work and out-of-work activities that may have led to the illness.
- Review the employee's work environment for potential COVID-19 exposure.

OSHA also recommends tracing the infected employees workplace contacts and testing those co-workers for coronavirus.

Recording claims: Only COVID-19 cases that were determined to have come from the workplace and required hospitalization or days away from work need to be recorded, according to the guidance.

It also states that if multiple employees in a particular business unit test positive, the assumption is that these coronavirus cases are work-related.

The takeaway

The new guidance is a lot to swallow, particularly as many employers do not have the expertise to conduct illness investigations.

OSHA stresses that it doesn't expect perfection, but that it does expect employers with more than 10 employees to conduct investigations as prescribed above, particularly interviewing the employee and investigating if others who work with them also contracted COVID-19.

IT'S LIKELY WORK-RELATED ...

- When several cases develop among workers who work closely together.
- If it is contracted shortly after lengthy, close exposure to a particular customer or co-worker who has a confirmed case of COVID-19.
- If a worker has frequent and close exposure to the general public in a locality with ongoing community transmission.

IT'S LIKELY NOT IF ...

- The individual is the only worker to contract COVID-19 in their vicinity and their job duties do not include having frequent contact with the general public.
- They closely associate with someone outside of the workplace who has COVID-19.

Given the nature of the disease and the ubiquity of community spread, however, in many instances it will be difficult to determine whether a COVID-19 illness is work-related, especially when an employee has potentially been exposed both in and outside the workplace.

There may also be a limit to the insurance claim period. Waiting periods are listed on your policy. ❖

More Workers Sue Employers over COVID-19 Issues

AS THE COVID-19 pandemic wears on and more employees go back to work, the risk of catching the disease for workers has spawned a growing wave of employment litigation.

Lawsuits are flying as employers struggle to keep their workplaces safe and negotiate an often-confusing mishmash of new and existing laws and regulations. Regulators have been issuing new rules for dealing with COVID-19 among workers, and Congress has passed laws addressing workers and the pandemic.

Law firm Ogletree Deakins reviewed court filings for March through May and found that COVID-19-related lawsuits fell into a number of categories. The list is instructive for any employer who has continued operating or has opened or is about to reopen operations after local stay-at-home orders are lifted.

Knowing what kind of actions are most prevalent can also help you devise strategies to avoid being sued in the first place.

Here are the types of claims, and the percentage of all COVID-19-related claims against employers that they account for:

40%: Whistleblowing, retaliation or wrongful discharge – These lawsuits will typically include allegations of retaliation for objecting to unsafe working conditions and exposure to individuals with COVID-19 symptoms in the workplace.

23%: Unsafe working conditions – Allegations usually include:

- That an unsafe workplace has caused sickness and/or death due to COVID-19.
- That an employer has failed to take appropriate measures to adequately clean and sanitize workplaces.
- That an employer has failed to provide necessary personal protective equipment, present adequate handwashing areas and sanitizing dispensers, or enforce social distancing protocols.

15%: Disability discrimination – Allegations usually include:

- Forced leaves of absence.
- Alleged failures to accommodate, including denials of requests to work from home.
- Faking leave due to COVID-19 concerns.

12%: Family and Medical Leave Act/Families First Coronavirus Response Act – Allegations usually include:

- Failure to provide leave related to COVID-19.
- Retaliation for utilizing leave related to COVID-19.

6%: Wage and hour – These lawsuits will typically include allegations of failure to pay for hours worked prior to closures due to COVID-19 concerns. These cases are expected to grow as more employees work remotely and workers spend time off the clock for temperature checks and health screenings at some firms.

The takeaway

Ogletree predicts that employee-initiated lawsuits that relate to COVID-19 will increase as states and local municipalities ease stay-at-home orders and more people go back to work.

The law firm has the below tips to reduce the risk to coronavirus-related employment lawsuits. ❖

AVOIDING LEGAL ACTION

- Keep policies up to date, particularly those related to harassment, discrimination, retaliation and the FMLA.
- Train managers, supervisors and HR staff on how to respond appropriately if employees make requests or express concerns regarding COVID-19 safety practices.
- Prepare a COVID-19 workplace safety plan and communicate and train your staff on the plan.
- If you are conducting health screenings, temperature checks or virus-testing, make sure that you do so safely by complying with social distancing requirements and with privacy laws in mind (you may want to consider having employees sign releases so they can't sue you for conducting the testing).
- Document the steps your organization takes if an employee tests positive for COVID-19. If you are changing employees' pay, make sure you give them notice of those changes in advance.
- If you are cutting staff, make sure you set uniform rules and criteria for who stays and who is let go or furloughed, in order to avoid claims of discrimination. Seniority, for example, is a good way to avoid discrimination allegations..