April 2014 Volume 2, Issue 8

Curry Insurance Agency

WORKERS' COMP

When You Can and Can't Discipline a Claimant

HERE'S A SITUATION you may want to avoid: disciplining workers who report workplace injuries.

It's against state workers' comp laws and could land you in hot water with OSHA. That's what happened recently to Ohio Bell Telephone Co., which the U.S. Department of Labor sued, accusing the company of violating whistleblower provisions of the Occupational Safety and Health Act of 1970 after it disciplined 13 workers who had reported workplace injuries.

The case illustrates what not to do if you have employees who file workers' comp claims, even if you suspect that they may be fraudulent.

The lawsuit, filed in U.S. the District Court in Cleveland against Cleveland-based Ohio Bell, accuses the phone company of issuing one- to three-day suspensions and/or issuing written disciplinary warnings against the workers.

The lawsuit cites the case of one worker who injured his back, shoulder and neck in January 2013, while loading boxes into his work vehicle at Ohio Bell. He sought medical treatment on Jan. 18, and was released back to work on Jan. 31, 2013.

Ohio Bell determined that he had violated its ergonomics policy and issued him a written disciplinary warning and assessed a one-day suspension, which he served on Feb. 12, 2013, according to the lawsuit.

The suit charges the company with violating OSHA's whistleblower provisions.

Besides OSHA's whistleblower protections, most states have laws that prohibit employers from disciplining workers for filing workers' comp claims. Depending on the state, the complaint can be filed inside or outside the workers' comp system and, in the case of the latter, it can open up the employer to punitive and compensatory damages.

In California, the effective law is Section 132(a) of the Labor Code, which makes it a misdemeanor for an employer to discriminate in any way, including discharge or threat of discharge, against an employee who has filed or is thinking about filing a workers' comp claim or an employee who has received a workers' compensation award. The employee who has been discriminated against is entitled to a maximum penalty of $10,000.

When you can administer discipline

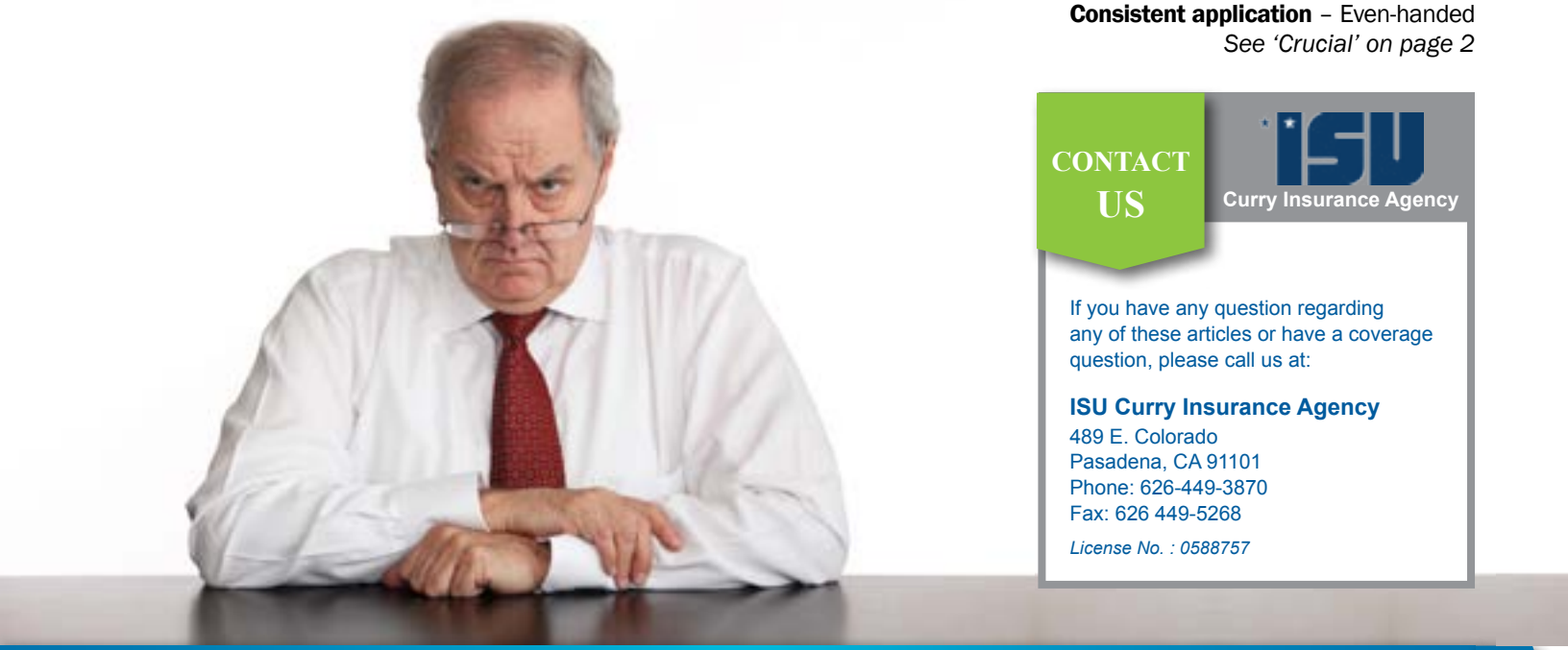
Administering discipline against someone who has filed a workers' comp claim can be tricky, but you should be protected if you have good cause, treat employees consistently, and have good documentation.

Good cause – To test whether good cause applies, you should balance management discretion with fairness to the employee.

One aspect of proving there was good cause can be to show that the behavior that spurred you to consider disciplinary measures was clearly against company policy. For example, is the infraction described in your employee handbook?

Consistent application – Even-handed

See 'Crucial' on page 2



CONTACT US

Curry Insurance Agency

If you have any question regarding any of these articles or have a coverage question, please call us at:

ISU Curry Insurance Agency
489 E. Colorado
Pasadena, CA 91101
Phone: 626-449-3870
Fax: 626 449-5268
License No. : 0588757

AFFORDABLE CARE ACT

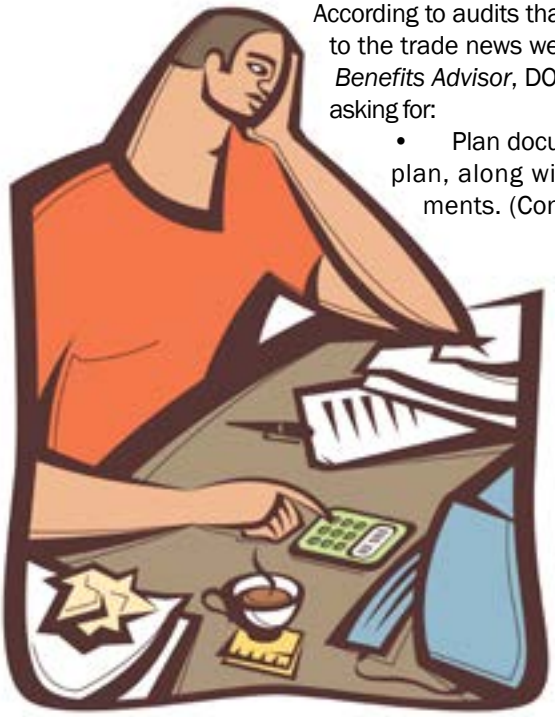
Be Prepared for the Inevitable: a DOL Audit

THE DEPARTMENT of Labor has said it wants to audit all employee benefit plans in the country by the end of 2015. While it may be hard-pressed to meet that goal, the DOL will be out in full force to audit employers' health plans to ensure they comply with the Affordable Care Act.

All employers that provide employee benefits to their workers need to be prepared when the DOL comes knocking.

During an audit, the DOL will review health and welfare plan documents and other plan materials. These are essentially compliance audits. They want to see if you have all of the correct documents and that you are administering those documents in a way that is consistent with federal laws and regulations.

The DOL will levy fines for non-compliance. According to audits that were reported to the trade news website *Employee Benefits Advisor*, DOL agents will be asking for:



- Plan documents for each plan, along with any amendments. (Content in all plan documents must comply with ERISA regulations.)
- Current summary plan descriptions.
- Form 5500 and accompanying schedules for the most recent plan year and previous three years. This form is used to file an employee benefit plan's annual information return with the DOL. It should include not only health plan information but also 401(k), IRAs, money purchase plans and stock bonus plans.
- A listing of all current service providers, and those from the past three years.
- All current contracts with administrative service providers on the plan, and most current fee schedules.
- All insurance contracts between plan and service providers.
- Name, address and phone number of the plan administrator.
- Sample HIPAA certificate of creditable coverage, and proof of compliance with on-time issuance of COBRA notices.
- Notice of special enrollment rights, and a record of dates when the notice was distributed to employees.
- Written eligibility criteria for plan enrollment.
- Documentation on all mandatory employee notices, i.e., ERISA Statement of Rights, Women's Health and Cancer Rights Act notice, etc.
- Copy of most recent monthly bill for premiums (if any) from insurance carrier(s).
- Copy of check, wire transfer or other methods of payment for insurance premium (if any).
- Enrollment form(s) for the plan.
- Employee handbook (if any).

Fines

The fines involved can add up quickly. And while the DOL does not publish a schedule of its fines, it was documented by Employee Benefits Advisor that breaches of ERISA reporting and disclosure requirements are penalised at $110 a day, per person.

And it notes that most fines for non-compliance under the ACA are not tax-deductible, either. ❖

Continued from page 1

Documentation is Crucial in Disciplining Employees

enforcement of the rules is critical to ensure that one employee is not punished more than others.

Failing to be even-handed can make it seem as though enforcement of the rules is only a pretext for the real reason for discipline: retaliation for the workers' compensation claim.

Consistent application is important. For example, even if the rule is in the handbook, the employee could argue that the rule was broken by everyone and enforced selectively against him.

Alternatively, if the rule was not in the handbook, it could be argued that the rule was made specifically for him as a means of discriminating against him.

Documentation – The golden rule of disciplining employees is documentation, regardless of whether they have a filed workers' comp claim.

Documentation is your evidence to back up the need for discipline.

If you don't have any evidence other than the supervisor's observations – even if the supervisor says that the misconduct has been consistent – do not proceed with terminating the employee.

To start the documentation process, advise the employee of the unacceptable behavior and give them an opportunity to improve. Document what you have told them and have them sign the agreement that they will improve their behavior.

If they don't, then you've got the start of documentation to be able to take further action later. Again, consistent enforcement of the rules is key.

Document infractions of all employees and supervisors – not just those of the employee in question. ❖

DATA SECURITY

Beware: California a Top Target for Cyber Crime

CALIFORNIA IS a major target of cyber crime in the U.S., accounting for one in six hacks into major computer systems in the country, according to a new report by the state Attorney General's office.

While the damages are in the billions nationwide from hacking attacks mostly on businesses, California by a large margin tops all states in the number of hacked systems, the number of computer systems infected by malware, the number of victims of Internet crimes, the losses suffered as a result of those crimes, and the number of victims of identity fraud, according to the report.

In addition, because of the outsized role new technologies and mass-media entertainment play in its information-based economy, California is particularly vulnerable when its networks become infected and its intellectual property is stolen.

In 2012, the Privacy Rights Clearinghouse recorded at least 331 breaches in the U.S. caused by international criminals who were purposefully trying to compromise databases or networks. California accounted for 17% of those breaches which, in turn, contributed to putting at risk the sensitive personal information of at least 2.5 million Californians that year, according to the report.

Between 2009 and 2012, the number of intentional breaches in the U.S. jumped by 280%, but during that same period the number of breaches in California shot up 560%.

The rapid increase in international breaches both in the state and nationwide should be cause for concern for any business that has an online presence, but particularly for those that have sensitive customer information online, like ID information and credit cards.

Cyber security best practices

Strong passwords – Use strong passwords and change them regularly. Passwords are the first line of defense in preventing unauthorized access to any computer. The more complex, the better, with a combination of characters, letters and numbers.

Install and maintain anti-virus software – The primary way that attackers compromise computers in the small office is through viruses and similar code that exploits vulnerabilities on the machine. You should train your staff on how to recognize a computer virus infection.

Use a firewall – Unless you have a database that is totally disconnected from the Internet, it should have a firewall to protect against intrusions and threats from outside sources. While anti-virus software will help to find and destroy malicious software that has already entered, a firewall's job is to prevent intruders from entering in the first place.

Secure socket layer – If you are handling credit card transactions, make sure that your payment system includes a secure socket layer to encrypt all of the important data of each customer.

Control physical access – Not only must assets like files and information be secured, the devices that your employee use must also be safe from unauthorized access. The single most common way that protected information is compromised is through the loss of devices themselves, whether through theft or accidentally.

Limit network access – Limit access to your most important data to only a few individuals in your organization.

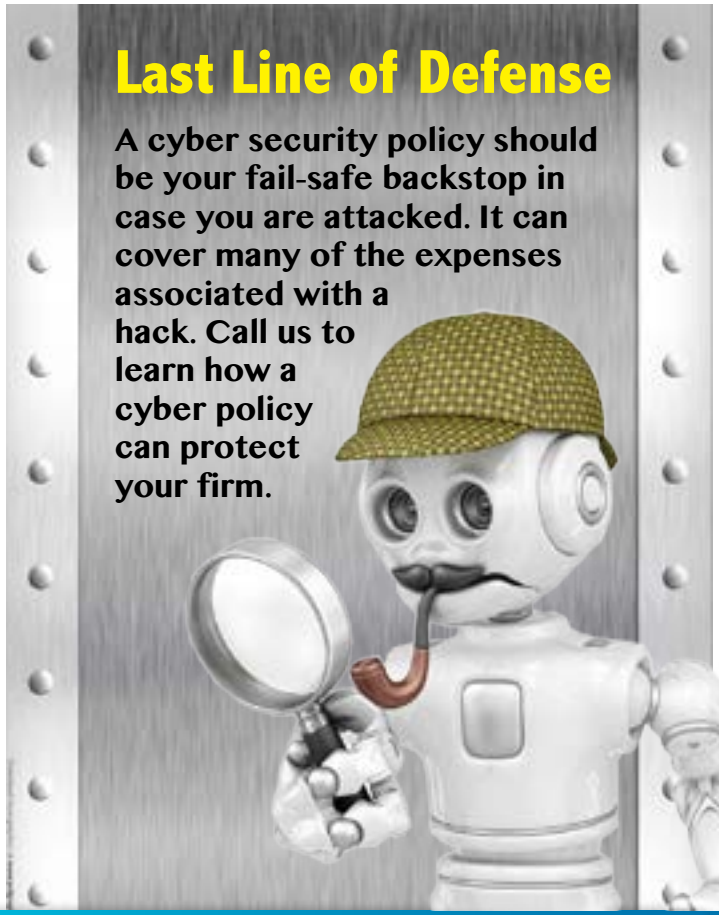
Plan for the unexpected – Natural or man-made disasters can strike at any time. Important health care records and other vital assets must be protected against loss. There are two key parts to this practice: creating backups and having a sound recovery plan.

Configuration management – New computers and software packages are delivered with a dizzying array of options, but little guidance on how to configure them so that the system is secure. In the face of this complexity, it can be difficult to know which options to permit and which to turn off. Here are some rules of thumb:

- Uninstall any software application that is not essential to running your business (e.g., games, IM clients, photo-sharing tools).
- Do not simply accept defaults or standard configurations when installing software. Step through each option, understand the choices, and obtain technical assistance where necessary.
- Disable remote file sharing and remote printing within the operating system configuration. Allowing these could result in the accidental sharing or printing of files to locations where unauthorized individuals could view them.

Protect mobile devices – Laptops, smart phones and portable storage media are even more vulnerable to hacking, making it easier for hackers to gain entrance to your company data. Because of their mobility, these devices are easy to lose and vulnerable to theft. Make sure they are protected, too.

Establish a security culture – None of the above measures can be effective unless your staff is willing and able to implement them, and you enforce policies that require these safeguards to be used. In short, you must instill and support a security-minded culture. ❖



HUMAN RESOURCES

Employee Drug Abuse Costs Employers Dearly

THE NATION'S drug abuse plague is costing employers some $81 billion annually due to employee illness, absences and lost productivity, according to a new study.

According to the National Council on Alcoholism and Drug Dependence Inc., 70% of the estimated 14.8 million Americans who use illegal drugs are employed, and workers who report having three or more jobs in the previous five years are about twice as likely to be current or past year users of illegal drugs as those who have had two or fewer jobs.

And now, with the changes in marijuana laws, employers are concerned that more people (read employees) will get hooked on drugs.

So far, 28 states have enacted laws on medical marijuana and two have legalized possession of small amounts of the drug.

Drug use, abuse or addiction by employees and members of their families can lead to a range of problems for business, such as lost productivity, absenteeism, injuries, fatalities, theft and poor employee morale, and increases in health care usage, legal liabilities and workers' compensation costs.

Some of the problems that drugs can cause in the workplace are:

- Sluggishness and impaired job performance.
- The employee setting up purchases or using drugs at work.
- Selling illegal drugs to or arranging purchases for co-workers.
- Psychological effects due to drug use by a family member, friend or co-worker that affects an employee's job performance.

Signs of drug use in the workplace

According to the council, the following job performance and workplace behaviors may be signs of possible workplace drug problems:

- Inconsistent work quality.
- Poor concentration/lack of focus.
- Lower productivity or erratic work patterns.
- Increased absenteeism or on-the-job "presenteeism."
- Unexplained disappearances from the job site.
- Carelessness, mistakes or errors in judgment.
- Needless risk taking.
- Disregard for safety for self and others.
- Extended lunch periods and early departures.
- Odd/socially unacceptable workplace behavior.

What can you do?

If you are concerned about drug abuse by your workers, you can establish an employee assistance program as well as a drug-free workplace program, which help refer your staff member enrollees and their families to community resources and services to help fight drug abuse.

Studies have found that employers with successful employee assistance and drug-free workplace programs reported improved morale and productivity, as well as decreases in absenteeism, workplace injuries and accidents, downtime and theft.

Long-term results can include better health among your employees and decreased use of medical benefits. ❖