

Risk Monitor



Risk Management Provider Reveals Data Concerning Top Construction Defects

The 10-year housing and real estate boom in this country has been a double-edged sword for the construction industry. While the top 100 U.S. homebuilders were reported to have sold an estimated 1,000 new homes a day in 2002, such performance isn't without a downside.

In the January 2004 issue, Consumer Reports noted that approximately 15 percent of all new homes built each year have serious problems. They place this startling statistic right at the doorstep of the building boom. The construction industry has been bombarded from all sides because of this phenomenon. Building defects have resulted in lawsuits costing the industry millions of dollars, general liability insurance costs are rising, and increasingly knowledgeable consumers are more critical of the finished product and more likely to sue.

On the heels of all of this, comes a survey of quality assurance data tabulated for the construction industry that proves leading construction defects are mostly the result of failure to follow building code requirements or installation instructions. And as if to add insult to injury, the survey goes on to show most of these defects are preventable. The survey completed by Quality Built, a provider in risk management and quality assurance services, used data gathered by their field inspectors during inspections of 31,995 completed homes and condominiums across 27 U.S. states for the 12-month period ending Oct. 1, 2005.

Single-family homes averaged \$5,398 in corrected defects per home while multi-family homes and mixed commercial use construction averaged \$4,556 in corrected defects. The survey also identified the leading risk items for each housing type. With regards to single-family housing, the top defects included:

- Building paper and house wrap installation flaws
- Improper framing around windows and doors

- Missing structural straps and connectors

Multi-family and mixed commercial use construction were most frequently cited for:

- Unprotected penetrations in life-safety assemblies
- Missing fire-rated materials at electrical device boxes
- Building paper and house wrap installation flaws

None of these defects are visible to a homeowner or building owner upon completion, but can lead to serious consequences and legal battles down the road. However, all of them can be easily corrected during construction if identified early through a quality assurance inspection.

Construction firms should take the following precautions to prevent a defect lawsuit:

- Hire a lawyer to get your contracts tightened up.
- Include Right-to-Cure, mediation and arbitration clauses as stopgap measures to prevent lawsuits.
- Find a set of national construction standards that you back and include them up front in your contract.
- Spend time going over the contract with the potential home buyer before they sign to make sure they understand what they're signing, and agree to the construction standards you've specified. If your attorney agrees, consider allowing clients three days to review the contract before signing, or three days after signing to cancel the deal.
- Create a small fact sheet or brochure for your clients that remind them of the key points of the contract – that you have the right to be notified first and granted the opportunity to fix the problem, the acceptable method for repair (included in the construction standards), and that mediation and arbitration are the next opportunities to resolve the issue prior to a lawsuit.

April 15th is ahead. The IRS warns consumers may be subject to a Tax Refund E-mail Scam. The faulty e-mail is from "taxrefunds@irs.gov," directing consumers to a link requesting personal information. This information is used to steal the taxpayer's identity & assets. Call our Benefits Department with questions at (317) 844-7759

TOBIAS
INSURANCE GROUP, INC.

Tobias Insurance Group, Inc.
9247 North Meridian Street, Suite 300
P.O. Box 90380
Indianapolis, IN 46290

Phone: (317) 844-7759
Fax: (317) 844-9910
Website: <http://www.tobias.com>



Show No Disparity When Dealing with an Aging Workforce

When employers think diversity, most think in terms of sociological factors such as race or religion. But there is another type of diversity that's becoming increasingly more prevalent in today's workforce and that is age diversity. As Baby Boomers continue to work well past normal retirement age, the phenomenon will become more widespread.

Having the wisdom and experience of a graying workforce population comes with a price. Under the ADEA, it is unlawful to discriminate against a person because of age with regard to any term, condition, or privilege of employment, including, but not limited to, hiring, firing, promotion, layoff, compensation, benefits, job assignments, and training.

This aging law was given a new lease on life with a recent Supreme Court decision. In the landmark case of *Smith et al. v. City of Jackson, Mississippi*, No. 03-1160, a divided Court, by 5-to-3, held that the ADEA authorizes disparate impact claims. The doctrine of disparate impact means that even where an employer is not motivated by discriminatory intent, Title VII prohibits an employer from using a seemingly neutral employment practice that has an unjustified adverse impact on members of a protected class. Of course, employees 40 and older are a protected class. The real Pandora's Box that was opened by this decision actually lies in the nature of the disparate impact suit itself because unlike disparate treatment claims, disparate impact claims don't require proof of discriminatory intent. Their emphasis is on whether or not a company's policies and practices adversely affect a protected group. The claimants must have substantive proof that the disparate impact exists; they can't just allege that there is the possibility that there may be a disparate impact resulting from the policy or practice. The downside here is that even though there may have been no discriminatory intent on the employer's

part, the fact that the disparate impact exists makes that employer legally liable.

What should employers be doing as a result of this heightened employment practices liability? The first response should be to review benefits, compensation and employment policies and practices to determine if there is any disparate impact on older workers. You will also need to perform a statistical analysis to prove the inaccuracies in the data of any potential claimant. A current statistical analysis will also evaluate whether there is the potential for disparate impact on older workers from a particular workplace policy or procedure in the future.

The next step you need to take is to talk to your agent about Employment Practices Liability Insurance (EPLI). Most comprehensive general liability policies exclude employment-related claims. Although a directors and officers policy may offer some form of protection, it won't cover the business entity itself. Other forms of insurance, such as fiduciary liability coverage, usually won't cover these types of claims either.

What an EPLI policy does is provide coverage for the cost of defending against and/or settling various types of claims, including discrimination, sexual harassment and wrongful termination. The majority of EPLI policies require the insurer to defend an employer against covered claims. The insurance company usually has the right to select the defense counsel. EPLI insurers typically have pre-approved, panel counsel hired to defend their clients. The cost of defense lessens the amount for settlement, so having an EPLI policy will actually encourage out of court settlements.

continued from page 4...Are You Legally Monitoring Your Employees' Electronic Communications?

company time.

- The Business Extension Exception – Section 2510(5)(a) exception also covers interception done in the ordinary course of business. It is similar in intent to the provider exception.

What all of these exceptions boil down to is that employers are justified in intercepting email messages as long as they have a valid business reason for doing so. However, if the business takes physical action to protect the privacy of email by installing a system that allows messages to be marked as confidential or by using passwords; or if the business tells

employees that their email is private, the employer's right to intercept may be considered voided unless one of the above stated exceptions can be proven.

Although there are still accusations that intercepting email is an outright invasion of a worker's privacy even though the message may be written on company time and using company equipment, intercepting emails is becoming increasingly necessary. As the number of employees who sue because of harassment that occurred via email increases, businesses will find that limiting risk will depend upon knowing when you can legally intercept.

Is Your Workers' Compensation Plan a Pork Barrel for Would-be Scammers?



Scamming “the man” can be a favorite pastime among some employees, and one of the best places to run a con is through your workers’ compensation plan. If you aren’t vigilant, a good scam artist can perpetuate the fraud for a very long time.

The most common garden-variety type of workers’ comp fraud is the phony workplace injury that’s discovered later, when the employee is accidentally caught doing heavy lifting or seen working for another employer while collecting benefits. Fraudulent claims can also occur when an employee complains of unseen ailments or extends the length of a legitimate claim because he doesn’t want to go back to work.

No matter what form it takes, everyone in the company feels the effects of workers’ comp fraud. Other employees may have to put in more hours to compensate for the lost productivity, or an employer may have to decrease the percentage of annual raises because of higher workers’ comp premiums.

How can you evaluate the potential for workers’ comp fraud at your company? These are some signals that will alert you to a possible scam in the making:

- If an employee has an accident shortly after arriving on Monday morning, this can be a sign of a scheme because the injury may have resulted from weekend activities.
- If an injured worker refuses treatment from a doctor or physical therapist, it could be cause for concern. Their reluctance to receive treatment could be an attempt to keep a phony injury from being discovered.

- If a disgruntled employee or one who knows they are about to be laid off files a workers’ comp claim, it may be a ruse to get even with the employer.

Of course, while it is important to be alert to possible fraudulent claims, it is far more important to prevent them from happening in the first place. According to the Coalition Against Insurance Fraud, there are several things you can do to combat workers’ comp fraud in your company:

- Verify references and background information carefully.
- Publicize your workers’ comp policy to all new and current employees, and provide them with updates at least once each year.
- Spread the word that money paid for fraudulent claims comes out of the employer’s pocket, and can directly impact salary increases for employees.
- Educate supervisors on workers’ comp issues, including how injuries decrease productivity and how costs affect the bottom line.
- Display fraud awareness posters and the National Insurance Crime Bureau’s fraud hotline number.
- Work with your insurer to implement a safety-management program that can eliminate possible safety problems.
- Be aware of workers’ comp fraud indicators when a claim is made.
- If you suspect a fraudulent claim and have evidence or witnesses to back up your suspicion, contact your insurer’s special investigations unit immediately.
- Pay attention to employee complaints and concerns about their working conditions. The strongest predictor of fraud is a chronically disgruntled work force.

Median Employment Lawsuit Damages Continue to Rise

According to the 2005 edition of *Employment Practice Liability: Jury Awards Trends and Statistics*, damages awarded for employment-related lawsuits were approximately 20 percent higher in 2004 than the year before. While actual damages rose, the percentage of plaintiffs winning their cases dropped slightly.

For 2004 the median jury award for employment-related lawsuits was \$218,133, compared to \$182,131 for 2003. The probability of a plaintiff winning their case continued to decline at 63 percent and has decreased seven points since hitting 70 percent in 2002.

Most awards were in the \$100,000-to-\$249,000 range (22 percent) and \$250,000-to-\$499,000 range (17 percent), according to the report.

A breakout of the various types of employment-related cases along with median awards follows:

Employment-Related Lawsuits

Type	Median Award
Whistleblower	\$270,000
Discrimination (Overall)	\$187,583
Age-Discrimination	\$262,405
Disability	\$211,272
Sex	\$186,250
Race	\$138,880
Other	\$101,563
Retaliation (Overall)	\$140,000
Wrongful Termination	\$125,880

Source: *Employment Practice Liability: Jury Awards Trends and Statistics, 2005*, Jury Verdict Research, Horsham, Pa.

Are You Legally Monitoring Your Employees' Electronic Communications?

Employees' right to privacy when using electronic communications has become a major workplace issue within the last decade. What constitutes an invasion of privacy? When does an employer have the right to monitor electronic communications? And does monitoring bring up the Orwellian image of Big Brother?

The Electronic Communications Privacy Act (ECPA) of 1986 is the only federal statute that deals directly with the interception of e-mail. The ECPA was enacted to extend an earlier legislation's protection against the unauthorized access of wire and oral communications to include electronic communications. Although the Act doesn't expressly mention e-mails, courts have interpreted the term "electronic communications" to include emails.

The ECPA does not, however, guarantee an employee's right to email privacy in the workplace. There are three specific instances when an employee's protection under the ECPA does not apply:

- The Consent Exception - Section 2511(2)(d) indicates that an interception of an electronic communication is considered legal if the person doing the intercepting is a party to the communication, or if one of the parties involved in the

communication consents. The only exception to this proviso is if the purpose of intercepting the communication is to use it to commit a crime or tort. If an employer asks their employees to sign an employment agreement stating that their electronic communications will be monitored, the agreement will nullify the protection of the ECPA.



- The Provider Exception – Section 2511(2)(a)(i) allows an officer, employee, or agent of a provider of wire or electronic communication service, whose equipment is used in the transmission of an electronic communication, to intercept, disclose, or use that communication in the normal course of employment if that person is involved in an activity which impacts upon the normal course of operations or upon the protection of their property rights. This means that intercepting emails to conduct quality checks is permissible as is intercepting them if you believe an employee is "stealing" the service by sending emails to friends on

continued on page 2

TOBIAS

INSURANCE GROUP, INC.

9247 North Meridian Street, Suite 300
P.O. Box 90380
Indianapolis, IN 46290

Phone: (317) 844-7759

Fax: (317) 844-9910

Website: <http://www.tobias.com>

Risk Monitor