HR insight
Proven strategies for the human resources professional
HRHero.com

September 2016
Vol. 13, No. 5

Highlights

Computing commuting time

by Connor Beatty

Ask anyone with a long daily commute, and he will agree that it certainly feels like the workday begins long before he steps inside the front doors of the workplace each morning. Under the Fair Labor Standards Act (FLSA), commuting time is not considered working time, although there are a number of exceptions to that general rule.

Properly compensating employees for travel time is often one of the most difficult wage and hour issues employers face. Whether an employee is paid for the time he spends traveling depends on the kind of travel involved and the particular employment circumstances. In general, the time an employee spends commuting between home and work isn't considered compensable work time, even for employees whose worksites change. Several exceptions may apply, however.

Facts

Recently, a Maine employer was forced to pay $52,000 in back wages to its employees when it was tripped up by one of the exceptions.

Paul G. White Tile Company is one of the largest flooring contractors in New England, with offices in Portland and Bangor as well as Stratham and Keene, New Hampshire. The company requires its workers to report to a company warehouse at the beginning of each workday, travel to the particular worksite, and then return to the company warehouse at the end of the day.

Although many of the worksites are close to the warehouse, employees can sometimes spend two or more hours driving to and from a particular worksite. The company didn't compensate its employees for their travel time to worksites. According to the U.S. Department of Labor (DOL), that practice violates the FLSA. The result: Paul G. White Tile Company agreed to pay its employees $52,000 in back wages.

FLSA scenarios

Most employers know that under the FLSA, employees must be paid at least minimum wage for all hours worked up to 40 hours per week and compensated 1½ times their regular rate of pay for any work beyond 40 hours in a week, unless they qualify for an exemption. However, there is often confusion about what constitutes "hours worked," especially when it comes to travel time. Here are a few different scenarios that may apply to your workers:

- **Typical daily commute from home to work.** Commuting time before or after the start of the workday isn't considered working time and therefore isn't compensable. This is true regardless of whether the employee reports to the same location for work each day or

continued on page 2 ▶

Editor's note:

As an HR professional, there are always numbers to track and keep up with. From vacation days to wage calculations, it's safe to say there will be math involved. While the *HR Insight* lead article encourages you to closely watch the numbers associated with an employee's commuting time, in the *HRIT* "Technology@work" column, David Kaufman discourages employers from monitoring the numbers on the scale, worrying about what employees weigh, and instead encourages the use of several technologies to help track fitness markers like diet, exercise, and heart rate. A number that might surprise you is the 250 percent increase in fines for failing to comply with notice-posting requirements—read more about that recent change in the "Agency insight" column on page 7. I hope this issue of *HR Insight* helps you ace your next HR math test.

Sincerely,

Celeste Duke, Executive Editor

HRinsight

Vol. 13, No. 5

HR Insight (ISSN 1548-4211) is published monthly for $347 per year plus sales tax by BLR®—Business & Legal Resources, 100 Winners Circle, Suite 300, P.O. Box 5094, Brentwood, TN 37024-5094
800-274-6774
custserv@blr.com
http://www.HRHero.com

Executive Editor: Celeste Duke

◀ *continued from page 1*

works at multiple jobsites. Additionally, otherwise noncompensable commuting time doesn't become compensable simply because the employee commutes in a company-owned vehicle, loads and transports ordinary equipment and tools, or performs other minimal activities infrequently.

- **Working during a commute.** An exception to the first example would be if the employee is able to perform job duties during his commute. Certainly, your employees shouldn't be reading and sending e-mails while driving! However, in some cases, it's possible to start the workday en route to the office. Employees may perform work while taking public transportation to the office or use their smartphones to dictate a memorandum or participate in a conference call while driving. Although commuting time is not compensable per se, an employee should be compensated if he performs work during his commute.
- **Working from home and then commuting.** If an employee performs tasks that would trigger the start of the workday before she begins her commute, the subsequent commute may be considered working time. A court is more likely to rule that a workday has begun when the employee performs job-related tasks regularly, and such tasks take up a significant amount of time. By contrast, minor tasks that take only a few minutes wouldn't be enough to trigger the start of a workday. For example, skimming through e-mails over breakfast would not trigger the start of a workday, but writing long, detailed responses to e-mails may. This issue has been the source of much litigation in recent years because it has been difficult for courts to articulate a black-and-white rule for employers to easily follow.
- **Commuting for a special assignment.** Another exception to the general commuting rule would be a scenario in which an employee typically works at a fixed location in one city but is given an assignment in another city on a particular day and returns home the same day. The employee should be compensated for the time spent traveling to and from the nontypical work location, although the employer could deduct the time he would usually spend commuting to the regular worksite. In other words, any extra time the employee spends commuting as a result of the special assignment should be counted as working time.
- **Commuting to a centralized meeting place.** This scenario describes the Paul G. White case. When an employee is required to report to a certain meeting place to receive instructions, pick up tools or equipment, or perform other work, any travel time from the meeting place to a subsequent worksite should be counted as working time. This is true regardless of the custom or practice in the industry.
- **Travel as a principal activity.** Travel that is part of an employee's principal job responsibilities, such as traveling from jobsite to jobsite, should be counted as working time.
- **Long-distance travel.** Travel that keeps an employee away from home overnight will be considered working time when the travel cuts across normal working hours. However, if the employee is traveling outside normal working hours and is simply a passenger (e.g., on a plane or train), the travel time doesn't need to be counted as working time.

Takeaway

As Paul G. White Tile Company learned the hard way, misclassifying working time can be a costly mistake for employers. However, it's becoming increasingly challenging to meet the FLSA's requirements given the way technology has reshaped both the workplace and the workday. When an employee checks his e-mail from home over breakfast, not only do you need to consider whether the time spent checking e-mail is compensable, but you also need to consider whether the employee has officially started his workday, making his subsequent commute compensable.

Because compensating employees for commuting time when they must travel to various jobsites can be confusing, it's advisable to consider the situation in some detail and develop a policy that is both compliant with the law and fair to the employee. Proper training and good policies can go a long way toward protecting you from liability.

An employment lawyer can help you comply with the FLSA by applying the specific facts regarding your workers to the general rules laid out in this article.

Connor Beatty is an attorney with Brann & Isaacson in Lewiston, Maine. He may be contacted at cbeatty@brannlaw.com.

Check this out

Responding to a data security breach

by Billy Hammel

If you have never had to respond to a data breach, consider yourself lucky. However, odds are, your data has been compromised and you simply don't know it yet. There are simply too many ways in.

Forty-seven states and most U.S. territories have laws addressing data breaches. Companies must comply with the laws of each state where individuals affected by a breach reside. That can create serious compliance challenges. Federal law also comes into play, especially if information protected by the Health Insurance Portability and Accountability Act (HIPAA) is compromised.

Generally, state laws specify when a data breach must be reported. Not all breaches are reportable, especially if the compromised information is encrypted. If a reportable breach occurs, companies usually must provide notice to all affected individuals, various state agencies, and third parties. Notice requirements have strict time frames that vary by jurisdiction. The fines can be crippling, especially for small and medium-sized companies.

Create an incident response team

The incident response team must be able to quickly investigate, classify, mitigate, and report potential data breaches. At a minimum, the team should include representatives from IT, your operations department, and HR. Adding general or outside counsel is also highly advisable, especially since it adds a layer of attorney-client privilege. Make sure the team knows when and how to call in an outside forensics examiner or other technical consultants. If your company does not have a forensics examiner, find one.

Draft an incident response plan

The incident response plan should prioritize identifying the threat, taking remedial measures (e.g., quarantining affected systems), and making an initial assessment of the breach, including whether customers' or employees' personal information was compromised. The plan should prompt a full investigation of the breach, require an assessment of potential risks, and specify methods for complying with mandatory reporting requirements that may have been triggered. Finally, the plan should provide for a thorough postincident review to address lessons learned.

Obtain data breach insurance

Data breach insurance policies are not expensive and typically cover fines, notification expenses, and legal fees. But insurance is not a substitute for security. Many policies require a security plan and have exclusions for substandard security features. Develop and follow a strict security and response plan, even if you have data breach insurance.

Vendor agreements

Companies may be liable for a breach of data in the hands of a vendor. Your vendor agreements should address minimum security standards, risk control and allocation, investigation and notice responsibilities, and indemnity. The agreements should require vendors to obtain data breach insurance coverage for themselves and any subcontractors.

Be aware of state laws

Most states have laws (only Alabama and New Mexico do not) that outline your obligations if you experience a security breach. Most of these laws require an employer to conduct in good faith a reasonable and prompt investigation when it becomes aware of a breach of the security of the system. If it is determined that personal identifying information has been or will be misused, most of these laws outline requirements for notifying individuals whose information was stolen.

Bottom line

Navigating state and federal laws is daunting. If a data breach is significant, a company could face a class action lawsuit by affected customers or employees or even lawsuits brought by shareholders on behalf of a corporation against company officers for breach of fiduciary duty for failing to adequately protect sensitive data and/or mishandling the litigation and enforcement ramifications of a breach. Ultimately, there is a lot at risk, so companies must develop adequate policies and procedures before a breach occurs, not when responding to a breach for the first time.

Billy Hammel is a partner in the Dallas, Texas, office of Constangy, Brooks, Smith & Prophete, LLP. He may be contacted at bhammel@constangy.com.

Q&A

Are dress codes one-size-fits-all?

by Brad Cave

Q Our office messenger has been showing up for work dressed in jean shorts, a long T-shirt, and a ball cap. We don't think he is dressing appropriately for our office setting, and we've talked to him about it. The problem is, we haven't been enforcing our dress code for other workers. For example, we've let some folks wear flip-flops and sleeveless shirts to work in warm weather, even though that isn't allowed under our policy. Can we discipline the messenger if he continues to dress inappropriately?

A As long as you aren't singling out the employee for his dress code violations on the basis of a discriminatory or retaliatory reason, you may still rely on your dress code and require that he comply with it. He could file a discrimination claim if he is in a different protected class from other employees who've violated the policy without receiving discipline. But such a comparison is helpful only if the other employees are "similarly situated."

Your best bet is to enforce your policy for everyone. Provide your entire workforce with a copy of your dress code, and inform employees that you will enforce it going forward. If anyone has a religious reason for not complying with the policy, he must notify you so you may consider possible religious accommodations. Absent such a request, though, you should hold all employees to the same standard, and they should face the same consequences for violating your policy.

Brad Cave is a partner with Holland & Hart, practicing in the firm's Cheyenne, Wyoming, office. He may be contacted at bcave@hollandhart.com.

Classifying workers in the gig economy

by Jacob Monty

Thanks to technology, the "gig economy" has expanded beyond musicians. Companies such as ride service Uber, lodging connector Airbnb, and errand service TaskRabbit form the modern gig economy. Companies in the gig economy provide a business platform—generally a mobile app—to connect potential workers with customers. The companies rely on workers who choose to earn money working gigs—a series of brief contract jobs. Workers check their smartphones for an opportunity to pick up a passenger or run someone's errands when it is convenient for them and with no repercussions for declining.

The gig economy provides valuable services to customers while giving work to the unemployed and workers who simply want to earn extra cash. However, the classification of gig workers is a nightmare for businesses. Determining whether a worker is an independent contractor or employee has always been a highly subjective analysis involving many different factors, including work instructions, training, set work hours, and the furnishing of equipment. Many jobs have factors that point to both independent contractor and employee status. Gig workers are even more difficult to classify. In a case involving Lyft, a ridesharing service, a federal judge stated, "The jury in this case will be handed a square peg and asked to choose between two round holes."

The flexibility that is integral to the gig economy's success is responsible for some of the difficulty in analyzing gig workers' status. For instance, an Uber driver might work a traditional full-time office job during the week and pick up a few passengers on weekends to earn extra cash. By contrast, another Uber driver could spend 40 hours per week picking up passengers and rely solely on the gig for income. Uber has no control over the drivers' choices, but the choices could affect a court or agency's determination of whether the drivers are independent contractors or employees.

The government and plaintiffs' attorneys attack

On February 15, 2015, the U.S. Department of Labor's (DOL) Wage and Hour Division (WHD) entered into a memorandum of understanding with the Texas Workforce Commission (TWC) to combat worker misclassification. Under the agreement, the WHD and the TWC share information and coordinate enforcement efforts. That means an investigation by one agency may lead to an investigation by the other agency. The TWC and the WHD also share information with the IRS. If the TWC finds that a company misclassified workers and requires it to pay unemployment insurance taxes (generally a relatively small penalty), the agency could pass that information to the IRS, which could assess a larger penalty.

Texas businesses take note: The TWC is being more aggressive than ever before. Tax examiners and hearing officers are analyzing the status of workers the TWC previously deemed independent contractors.

Plaintiffs' attorneys are also joining the action. In addition to receiving a boost from the DOL, which launched a Web-based portal in September 2014 that allows workers to fill out intake forms that are sent to local attorneys, plaintiffs' lawyers are filing lawsuits on their own. Uber drivers have filed a class action lawsuit in California requesting reimbursement for gas and vehicle maintenance. DoorDash, which provides on-demand food-delivery services, has been sued by its drivers for alleged misclassification.

Ideas on how to resolve the uncertainty abound. Alan Krueger, former chief economist to President Barack Obama, and Seth Harris, former deputy labor secretary, support the creation of a new intermediate worker category. A California bill would allow independent contractors who depend on a business platform to collectively bargain with the company that operates the app without an official union and without being classified as contractors.

What should companies do?

First, evaluate your goals. Do you want to have control over your workers? Do you need to be able to assess their performance and make decisions accordingly? Will an independent contractor salesperson be effective without using your company's business cards and e-mail system? Instacart, a grocery-delivery service, recently reclassified its workers as employees. The change has reduced turnover, improved service quality, and lowered costs because Instacart can require employees to stay at a grocery store rather than paying independent contractors to drive to a store for each trip. However, the additional costs of hiring employees (e.g., healthcare benefits, workers' compensation insurance, and overtime) will not work for every business model.

Second, consult an employment attorney to ensure you are minimizing liability by treating your contractors like contractors, not employees. For example, to protect workers' independent contractor classification, do not provide them business cards or e-mail addresses. Do not pay for their training or business expenses, and do not stop them from working for competitors. Enter into independent contractor agreements, and require contractors to carry their own liability insurance. Do not require full-time work. If those restraints do not align with your goals for your contractors, go back to step one and reevaluate.

Finally, be aware of your options. If the tide is turning against your industry or the workers you classify as independent contractors, consult an employment attorney to see how you can minimize your liability. For instance, the IRS's Voluntary Classification Settlement Program allows employers to voluntarily treat contractors as employees for future tax periods. In return, employers pay only 10 percent of the employment taxes for the most recent tax year and no interest or penalties. That's an enormous reduction in the amount that would be due if the IRS acted first. To successfully combat the government and plaintiffs' attorneys on this hot-button issue, you must be prepared.

Jacob M. Monty is the managing partner of Monty & Ramirez, LLP, practicing in the firm's Dallas, Texas, office. He can be reached at jmonty@montyramirezlaw.com.

Check this out

DTSA gives employers new options to combat trade secrets theft

by Elijah Yip

Whether it's the secret recipe for your gourmet cupcakes or a unique process for manufacturing your best-selling product, trade secrets are a valuable company asset. When an employee leaves, there's a risk she will take your trade secrets with her to a competitor or use them to start her own business. So what relief is available if you're a victim of trade secret theft?

On May 11, 2016, President Barack Obama signed the Defend Trade Secrets Act (DTSA), which contains important provisions affecting employers of all sizes. The DTSA authorizes an employer to bring (and be subject to) suit in federal court for trade secret misappropriation, including misappropriation occurring outside the United States, and obtain a broad range of remedies. The DTSA also includes important provisions governing employer obligations and employee rights with regard to trade secrets, and extends those obligations and rights beyond traditional employees to contractors and consultants. Here are the highlights of the new law:

- **What does the DTSA do?** The DTSA creates a new federal remedy for trade secret misappropriation. Before, federal law criminalized only certain misappropriations of trade secrets. Now, the DTSA allows victims of trade secret misappropriation to sue in federal court.
- **Is the DTSA my exclusive remedy?** No. The DTSA creates a national standard for trade secret law and gives you more options for seeking relief, but it doesn't preempt state law. You may still take advantage of trade secret protections under state laws like the UTSA.
- **What's so special about the DTSA?** One feature of the DTSA allows a court to grant an "*ex parte* seizure order." Under this new remedy, trade secret owners may seek a court order to seize allegedly stolen trade secret items in the accused wrongdoer's possession without first giving him notice. Seizure orders are granted only in "extraordinary circumstances." To safeguard against the abuse of seizure orders, the DTSA entitles victims of wrongful seizure to damages, punitive damages in cases of bad faith, and attorneys' fees. It remains to be seen how courts will apply the *ex parte* seizure provisions of the DTSA and how often the remedy will be used.
- **What do employers need to know about the DTSA?** Injunctive relief granted under the DTSA may not "prevent a person from entering into an employment relationship" and must be consistent with state law "prohibiting restraints on the practice of a lawful profession, trade, or business." In other words, the DTSA doesn't override state law governing noncompete agreements. Claims under state law may need to be included in a lawsuit to enforce noncompete provisions in an employment agreement. The DTSA also provides immunity for whistleblowers (which the Act defines broadly to include independent contractors and consultants) who disclose trade secrets to any government official solely for the purpose of reporting or investigating a suspected violation of law or in a court filing made under seal. Notice of the whistleblower immunity provisions must be given in every agreement entered into after May 11, 2016, that restricts an employee's use of a trade secret or other confidential information. The notice requirement may be satisfied by referencing the immunity provisions in a policy document (like an employee manual) rather than inserting the provisions into each employment agreement.

For more specific information on how the DTSA affects you, consult experienced legal counsel.

Elijah is a partner with Cades Schutte LLP in Honolulu, Hawaii, and chair of its digital media and Internet law practice group. He may be contacted at eyip@cades.com.

Q&A

Does Brexit affect you?

by Elaine Young

Q What is "Brexit," and how does it affect my employees?

A "Brexit," a term combining the words "Britain" and "exit," was coined to describe a referendum in which citizens of the United Kingdom of Great Britain and Northern Ireland—sometimes shortened to UK or Britain—chose whether to remain in the European Union (EU) or leave it. On June 23, voters chose to leave the EU. While it may take a couple of years for Britain to separate itself in the most meaningful ways from the EU, there were immediate adverse reactions in the global market and much confusion over what Brexit means.

For U.S. companies sending U.S. citizens to the UK, there shouldn't be too much of a difference in terms of workers' ability to get a work visa, and they will still be allowed short-term visa-free travel to EU countries for business and tourism. However, voter opposition to the EU's "open borders" immigration policy, which permits any EU citizen to reside and work in another EU country, was a major reason for the Brexit vote, especially in light of the recent refugee crisis. U.S. multinational companies should therefore expect to see significant changes in UK immigration policy. Most likely, the changes will affect U.S. companies' ability to employ EU workers through a UK affiliate, transfer EU workers in and out of the UK, and deal with cross-border Social Security issues for Americans working in the UK and EU countries.

Elaine Young is an attorney with Kirton McConkie in Salt Lake City, Utah. She may be contacted at eyoung@kmclaw.com

Policy pointers

Don't give thieves access to your computer systems

by Sam Karson

In April, the U.S. Department of Homeland Security's (DHS) Computer Emergency Readiness Team issued an alert about new vulnerabilities in Apple's QuickTime software for Windows users. Recently, hackers started targeting HR professionals.

Don't ignore the front door

While it is important to stay abreast of the latest updates regarding cracking (breaking into computers for criminal gain) and back door vulnerabilities, HR professionals must stay focused on the front door. Many computer criminals use "spoof" e-mails to trick employees into letting them walk through the figurative front door. This is called "phishing." A common phishing scheme involves e-mailing an HR employee whose contact information is posted on the company's website or the employee's LinkedIn account. The e-mail address is similar or identical to that of a company executive whose contact information is also online. The fraudster requests proprietary business information or employees' personal information. A recent phishing scheme involved fraudsters posing as company executives and requesting employees' W-2 forms, which include sensitive information that could be used to steal employees' identities.

Information has been stolen. Now what?

If your employees' information is compromised, the first thing you should do is get in touch with an expert. How you respond to a data breach will have a significant impact on your company's liability and the damage that results from the breach. Employees must be notified of the breach. Keep employees updated throughout the process so they can take steps to protect themselves from identity theft.

The next step is to assess the scope of the data breach. Depending on what kind of information was stolen or accessed and how many employees are affected, you may have to notify the state government and credit reporting services. Most states have laws requiring companies to notify the state attorney general's office and credit reporting agencies when a data breach occurs. Each state's notification law is different in terms of what type of breach triggers the notification requirement and what information must be included in notifications, so it is important to familiarize yourself with the notification laws in states in which you operate. If medical information is involved, the Health Insurance Portability and Accountability Act may apply.

Finally, work with your IT staff to fix system vulnerabilities and improve your system security going forward.

Protecting your company from phishing attempts

The most effective way to protect your business from phishing is to make employees aware that phishing attempts are real and often involve fraudsters impersonating company employees. Ensure that employees are trained to detect phishing attempts. Most important, if an employee receives a request for personal information, he should call the person asking for the information to confirm the request. Also, employees should watch out for anything that doesn't look quite right, such as irregularities in e-mail addresses, strange wording, or requests that are seemingly out of the blue. You may want to adopt policies requiring that all personal information be shared using encrypted methods, such as ShareFile, SecureZIP, or TrueCrypt. Many strategies for guarding the front door involve commonsense operational security.

Bottom line

Cyberattacks will become more prevalent and more sophisticated, but HR professionals can decrease the risk of exposing employees' personal information to fraudsters by staying up to date on the latest threats, training employees regularly, and implementing commonsense operational security policies.

Sam Karson is an attorney with Brann & Isaacson in Lewiston, Maine. He may be contacted at skarson@brannlaw.com.

Pop quiz

The EEOC, ADA, and your wellness program

In last month's *HR Briefing*, we covered the Equal Employment Opportunity Commission's (EEOC) new final regulations on the Americans with Disabilities Act's (ADA) requirements for wellness programs offered by employers. Test your knowledge on these new regulations by deciding if the following statements are true or false.

1. Employers must provide notice to employees about the scope and use of medical information collected as part of a wellness program that makes disability-related inquiries or requires medical exams. **T** or **F**
2. Asking about tobacco use is not a disability-related inquiry, so screening for tobacco use doesn't trigger the application of the ADA's requirements for wellness programs that require a medical exam. **T** or **F**
3. The new rules apply only if the wellness program is limited to employees enrolled in the employer's group health plan. **T** or **F**
4. Employers can fulfill the final regulation's notice requirement either by paper or electronically. **T** or **F**
5. The final ADA regulations clarify that the 30% rule applies to only financial incentives provided in connection with the wellness program. **T** or **F**

Now, turn to page 8 for the answers.

Check this out

What HR must know before seeking background checks

by Kevin J. Skelly

The federal Fair Credit Reporting Act (FCRA) imposes obligations on employers that rely on certain background checks to make employment decisions. A recent class action lawsuit filed in federal court should serve as a wakeup call for employers on the many pitfalls associated with conducting background checks on job applicants and employees.

Applicants sue for FCRA violations

In April 2016, a class of former job applicants sued trucking company J.B. Hunt Transport Inc., alleging it violated the FCRA by obtaining credit reports on applicants without their authorization and without providing the necessary disclosures. According to the complaint, the application didn't contain any notice informing applicants that the company would obtain a background check as part of the application process.

The company allegedly failed to obtain an applicant's consent before obtaining a background report on him. He alleges that the background report contained incorrect information and the company disqualified him based on the inaccurate information. The putative class includes thousands of other individuals who applied for jobs. They are seeking damages of $100 to $1,000 per class member per violation, along with other damages.

Protections under the FCRA

The FCRA and state laws apply to employers that acquire background checks ("consumer reports") through third-party companies that are in the business of compiling background information ("consumer reporting agencies"). Consumer reports typically include information about an individual's creditworthiness, character, reputation, criminal background, driving record, and any civil lawsuits he has been involved in, among other information. The FCRA and many state laws contain various notification and consent requirements.

Before requesting a consumer report on an applicant or employee, an employer is required to provide him written notice that it might use information in the consumer report to make employment decisions. The notice must be a stand-alone document, not in an employment application. Employers must get the applicant's or employee's written authorization to obtain the consumer report.

If the employer decides to take an adverse action based on negative information contained in the consumer report, the FCRA and many state laws impose additional notification requirements. Under the FCRA, *before* the employer takes the adverse employment action, it must give the applicant or employee (1) a copy of the consumer report and (2) a written description of his rights.

If the employer decides to take adverse action based on information in the consumer report, it must give the applicant or employee notice that includes:

1. The name, address, and phone number of the consumer reporting agency that supplied the report;
2. A statement that the consumer reporting agency did not make the adverse action decision and cannot give specific reasons for it; and
3. A notice of the individual's right to dispute the accuracy of the information contained in the consumer report and his right to obtain, upon request, an additional free report from the consumer reporting agency within 60 days.

An employer that violates the FCRA is subject to actual damages suffered by the applicant or employee, along with attorneys' fees and costs. For willful violations, an employer is also subject to fines up to $1,000, plus punitive damages, attorneys' fees, and costs. Although the penalties associated with a single violation of the laws aren't substantial, violations typically involve a large number of individuals. Moreover, FCRA claims are often brought as class actions.

Bottom line

The FCRA and state laws contain many technical and procedural requirements that employers can easily overlook. Carefully review your procedures to ensure compliance.

Kevin J. Skelly is an attorney with Day Pitney LLP, practicing in the firm's Parsippany, New Jersey, office. He may be contacted at kskelly@daypitney.com.

Agency insight

Posting penalties go up 150%

by Joe Lavoie

The Equal Employment Opportunity Commission (EEOC) has issued a new rule that increases the maximum penalty for violating certain federal notice-posting requirements. Effective July 5, 2016, the new rule from the EEOC raises the maximum fine for failing to comply with notice-posting requirements from $210 to $525 per violation.

Employers must post in "conspicuous locations" notices that describe employees' rights under Title VII, the Americans with Disabilities Act (ADA), and the Genetic Information Nondiscrimination Act (GINA). Those laws are summarized in the U.S. Department of Labor's (DOL) "Equal Opportunity Is the Law" poster, which can be downloaded and printed without charge at www.dol.gov/ofccp/regs/compliance/posters/ofccpost.htm.

While the EEOC encourages employers to post the notices on their websites, the most conspicuous electronic posting means nothing if physical notices are missing.

The new rule raised the maximum fine without the traditional notice and comment period afforded under the Administrative Procedure Act. The EEOC was able to circumvent the notice and comment period because the new rule is mandated by the Federal Civil Penalties Inflation Act of 2015 and the inflation formula is prescribed by statute.

Joe Lavoie is an attorney with Sulloway & Hollis, P.L.L.C. He may be contacted at jlavoie@sulloway.com.

Last word on HR

All work and all play

by Mark I. Schickman

The relationship between work and leisure time has shifted dramatically in all directions. As often discussed in these pages, personal time has been invaded and conquered by the ubiquitous smartphone, which allows employee access 24/7. Waiting 15 hours to respond to an e-mail you received during dinner is way too slow by modern instantaneous standards.

At the same time, personal time has permeated the workplace in many ways. Gone are most employment policies that prohibit personal e-mails or computer access at work. Policies now grapple for terms, permitting "sporadic use" or outlawing phone use that "causes disruption" or "disrupts normal workflow." It has become unreasonable to ban all use of personal devices at work. If you think your employees will follow such a policy, you are wrong. So what is the best balance, and how do you reach it?

I work pretty hard and always look to see how leisure time can invade my day. A standing offer to my clients is a $50 discount off my hourly rate if I can schedule to take a call while on my deck. I'll cut my hourly rate in half for any client meeting we can hold while walking along the Bay trail that runs for miles past my office.

One $20,000 toy after which I have always lusted is the Seven Person Meeting Tricycle sold by Hammacher Schlemmer (www.hammacher.com/Product/124090). The 400-pound trike is 8 feet long, 6 feet wide, and 4 feet high and has the meeting leader steering in the center while the other six pedal and face the leader. Build camaraderie, get exercise, and conduct a meeting all at the same time. This was my favorite 20th century idea of how to mix business with recreation.

Recognizing that almost a quarter of all employees work off-site about 25 percent of the time, social work locations have grown, too. Fastcompany.com reports that many employees schedule several "coffee shop days" each month—saying they are more productive and experience fewer distractions from that change in environment.

Work in, work out

Health clubs have now become a new off-site work location of choice. *The Wall Street Journal* reports that high-end health club Equinox has carved out 1,150 square feet of computer workspace in its San Francisco SOMA location, and to meet demand, it's expanding that space to 6,000 square feet. It plans to create similar workspaces in its 80 other locations.

These Equinox member workers say that the combination of working and working out increases productivity—ideas come quickly while exercising, they can quickly run to a computer station to capture the work product, and then they return to the exercise regimen.

I often try to analyze what motivates employees, what makes them tick. For a generation, the most frequent answer was money, and then it was job satisfaction. More recently, the highest motivators have been the ability to take time off and the degree to which one's ideas were considered and implemented.

Today, the key to job satisfaction seems more holistic. A recovered economy and lack of city-center housing have created nightmare commutes throughout urban and suburban California. The number of people who never go to an office and the number who spend significant parts of their workweek away from the office are exploding. Work can be done seamlessly from almost everywhere. These factors are redefining the limits of what can be done to promote employee satisfaction. Nobody knows how this will ultimately work out—will it lead to an unsatisfying, never-ending cycle of work/play or to a joyful mix of playful work? Or will it create a gray mass that embodies neither satisfactorily?

Brian Dyson, former COO of Coca-Cola, describes life as "a game in which you are juggling five balls in the air—work, family, health, friends, and spirit. . . . You'll soon understand that work is a rubber ball. If you drop it, it will bounce back. But the other four balls are made of glass." There is a danger in conflating work with life, no matter how lifelike work becomes. Maintaining that satisfying separation—not just balance—might be the key to modern industrial relations.

Mark I. Schickman is a partner with Freeland Cooper & Foreman LLP in San Francisco, California. He may be contacted at schickman@freelandlaw.com.

Quiz answers

Here are the answers to the quiz on page 6.

1. **True.**
2. **False.** Merely asking about tobacco use is not a disability-related inquiry, but screening for tobacco use would trigger the application of the ADA's requirements for wellness programs that require a medical exam.
3. **False.** The rules apply without regard to whether the wellness program is limited to employees enrolled in the employer's group health plan.
4. **True.**
5. **False.** The final ADA regulations clarify that the 30% rule applies to any financial or in-kind incentive provided in connection with the wellness program.

HRHero.com

As an *HR Insight* subscriber, you have access to the HRhero.com Employers Forum (http://www.hrhero.com/forums/), where you can ask other HR professionals for help with your hardest dilemmas and offer your insight as well. If you have any questions or comments about the forum, contact Celeste Duke at cduke@blr.com.

Coming next

Is it legal to have a policy requiring employees to speak English when they're talking with other employees and around customers unless a cus-tomer doesn't speak English? Find out in the next issue of *HR Insight*.

HR it

A quarterly update on technology from HR Insight

HRHero.com

September 2016

HR hot byte!

Phishing for failure: avoiding scams. Ginni Rometty, IBM Corp. Chairman, President, and CEO, commented, "[Data] is the world's new natural resource. It is the new basis of competitive advantage, and it is transforming every profession and industry. If all of this is true—even inevitable—then cyber crime, by definition, is the greatest threat to every profession, every industry, every company in the world."

In many cases users, including your employees, are letting the bad guys in by opening attachments or visiting compromised websites. They may be enticed by an e-mail that seems innocent or work-related. The international business consortium Anti-Phishing Working Group estimates that between October 2015 and March 2016 the number of phishing websites jumped 250 percent. But how can you tell if an e-mail is likely a phishing attack?

Spelling and grammar: Most corporations have proofreaders to ensure communications aren't cluttered with misspellings and bad grammar. Most phishing scams lack a professional proofreader. Look for awkward phrasing and glaring misspellings.

Bad e-mail address: If an e-mail is coming from a large company or a government agency, it won't have a Gmail or Yahoo mailbox. Also, the site is the name directly next to the .com, .org, etc. Therefore, postoffice.badguys.com is not a U.S. Postal Service address.

Weird website: Before you click on a link, hover over it to see the hyperlink. If it takes you to a badguys.com site, don't click on it.

Too good to be true: You know the old saying—if something looks too good to be true, it's not true. An e-mail offering something for free, at a spectacular discount, or some other amazing incentive should be viewed with great suspicion.

I didn't order anything: Many scams ask you to click a link to check the status of something you ordered or some other offering you weren't expecting. If you don't recognize it, ignore it.

Chasing health at work using technology: wearables, apps, and more

An employer's bottom line is positively affected by improved employee health. In a 2014 study published in the *American Journal of Health Promotion*, scientists found that a morbidly obese employee on average costs an employer more than $4,000 more for health care and other costs than an employee of normal weight. They concluded, "For example, someone who is overweight or obese and also has diabetes is more likely to file a short-term disability claim compared to someone who doesn't have diabetes but is overweight or obese." Other studies give estimates for huge employee savings, billions of dollars, from reduced absenteeism and fewer accidents as a result of healthier workers.

The Centers for Disease Control found that in 2015, 30.4 percent of adults older than 20 are obese (a body mass index (BMI) of 30 or greater). There are reasons to believe the trends will be hard to manage—and work has a lot to do with it. According to the American Heart Association, "Sedentary jobs have increased 83% since 1950; physically active jobs now make up less than 20% of our workforce. In 1960, about half of the US workforce was physically active."

Catch 'em all or lock it down?

See page 3.

Fidelity Investments estimates that 80 percent of employers in the U.S. are doing something to help their employees get healthier, spending an average of $693 per worker. Many are deploying a new generation of technology to help their workers get fitter and stay healthier.

Wearable devices

Look around and you will see many, many folks wearing new types of bracelets—electronic ones. Special smartwatches, too. A study by analyst eMarketer estimated almost 40 million U.S. adults wore devices, including smartwatches and fitness trackers, last year—up 57.7% from 2014. The study estimated that by 2018, the ownership will jump to 81.7 million users. Trackers are being used to keep tabs on myriad parameters of the user's physical activity—from how many steps you take to how long you sleep.

FitBit is going after corporate health in a big way, starting a new initiative that uses the trackers as the foundation of corporate wellness. A FitBit executive commented, "With corporate wellness, we've already shown that our connected platform can drive higher engagement and better health behaviors in companies and communities. We've already begun expanding the reach of our technology through other channels, such as health plans."

Wearable technology also is being designed into many more products, like shoes. Research firm Tractica estimates that by 2021, more than 24.7 million smart-clothing products will be purchased each year. The firm also sees an expansion of uses as the research director explained, "Advanced sensor technology, miniaturization of hardware, and smart artificial intelligence algorithms will help

continued on page 2 ▶

bring wearables into the forefront of the fight against chronic conditions like diabetes, heart disease, and cancer. Expect to have your smart watch warn you about a stroke or heart attack, days in advance, which is when wearables will start to be taken much more seriously."

Applications

Employers don't necessarily need to invest in new hardware to help their employees become fitter. Using smartphones and desktops that they already have, employees can do quite a bit to monitor and improve their own health.

Calorie counters. Applications like MyFitnessPal (MFP), which have users logging what they consume in an electronic food journal that automatically converts the food entries to calories, are very effective. The developers of MFP claim to have 5 million foods in their database. The app has a fitness tracking component, too.

Get moving. Sitting too long is highly correlated with lots of bad health outcomes. There is a whole class of applications that encourage workers to get up and move around. The breaktimers send sound cues at appropriate intervals to encourage you to stand up. **Move** reminds you to stand up and provides exercises you can do in your workplace.

Sleep tight. A good night's sleep is also a critical part of health. **Sleep Cycle** advertises itself as "An intelligent alarm clock that analyzes your sleep and wakes you in the lightest sleep phase—the natural way to wake up feeling rested and relaxed."

Protect your eyes. Staring at a computer screen can be bad for your eye health. **EyeLeo** "reminds [you] to take breaks regularly, shows you simple eye exercises and prevents you from using computer at break times." The app **f.lux** "makes the color of your computer's display adapt to the time of day, warm at night and like sunlight during the day." In addition to eye health, the designers claim it can help you sleep better by adjusting your exposure to blue light.

Sit better. Bad posture can seriously affect your body—especially if you are sitting at a desk for 8 to 10 hours a day. Several apps use vibrations to force you to sit up straight. **Posture Man Pat** uses a computer's webcam to monitor posture and then notifies you if you are slouching.

Social tools

A Northwestern University survey found "people can do very well at losing weight with minimal professional help when they become centrally connected to others on the same weight loss journey." Of course, in a work setting some of this gets more complicated. Sharing your weight loss or your daily exercise results with your friends is one thing—but sharing with your coworkers is a whole additional layer of complexity. Employers should consult with their employment counsel before embarking on any effort where employee results are collected and/or shared. Clearly, employees must opt-in to participate and employers must be transparent in how they collect, store, analyze, and disseminate the results.

continued on page 3 ▶

Workplace wellness: tech tools

Wearables

Bands and other devices that track steps, sleep, and more. Next up: Smart shoes and clothing.

Applications

Count calories, get moving, protect your eyes, improve your posture, sleep better—all on your phone or desktop.

Social tools

People lose more weight and exercise more when there is a social component, but consider the privacy issues before starting.

Training & service delivery

Use your existing training platform and new food delivery sites to bring healthy living right to your employees.

◀ *continued from page 2*

Training and service delivery

There are thousands of training videos that employees can use to improve their physical fitness and overall health. To that end, employers are using their training portals and platforms to educate their employees on these other important life skills. Plus, there are videos on healthy food preparation.

Working late? That can lead to ordering something unhealthy. Some employers use sites that make it easy for their employees to order healthy food. Online food delivery company **Grub Hub** encourages restaurants to focus on healthy eating by "tak(ing) the complexity out of your menu by instead highlighting healthy ingredients that appeal to healthy diners, such as fruits, dark leafy greens, vegetables, omega-3 fats and whole grains."

Diettogo offers a Corporate Wellness Program that allows employers to provide "convenient, healthy and portion-controlled meals that can have a positive impact on their personal lives and productivity" both at home and at work.

Beyond bricks and mortar

Employers that are grappling with the reality that their employees are getting heavier and less healthy have plenty of options to help battle the bulge. Fortunately, especially for smaller employers, many of the tools now take the form of a simple band on your employees' wrists or an app on their computer.

❯ Hot byte!

Pokémon GO(es) to work

Add Pokémon GO to the digital distractions list that includes online shopping, updating Facebook, and watching YouTube. Given the game's amazing popularity, your employees are very likely to be playing the new video game phenomenon while on the job. According to Survey Monkey, in less than a week after the game's July 6 launch, it "attracted just under 21 million daily active users in the United States, surpassing Candy Crush Saga's rumored peak US smartphone audience of 20 million and making it the biggest mobile game in US history." At one point, the game had more users than Twitter.

Unfortunately, the game's popularity and the nature of play has created a huge number of accidents and left players susceptible to crime, including murder. In case you don't know how it is played, *Rolling Stone* explained it as, "It's still a Pokémon game, and has roughly the same principles as every other Pokémon from the past 20 years. You look for the critters, catch them, train them and battle with them. What's different here is that it uses the real world to inform your game experience…In order to interact with them, you need to actually walk to a particular place, like, in the real world. You can look at the game world through your phone's display, which serves as a viewfinder that mixes reality with game objects."

That is called "augmented reality" and is driving folks to pay close attention to the reality on the screen and not the reality they really are in. According to *Time*, "While in the throes of the Pokémon Go hunt, players have crashed cars while driving, gotten hit by cars while crossing the street, and been robbed because they weren't paying attention to their surroundings. Players have even fallen off cliffs without noticing until it was too late."

Of course, the popular game is spreading into the workplace. Airplane manufacturer Boeing had to ban the game last month after an incident. A leaked internal memo from the company reported by *Slate* stated, "Due to the popularity of Pokémon Go and users not being able to make the conscious decision to not play Pokémon at work—we had a near miss for a user getting hurt while playing the game. Due to that, we had to react and disable the Pokémon app from all devices—we had over 100 active installs of that application." The Pentagon also disabled the game from all government-issued devices saying, "taxpayers would appreciate government phones being used for government business."

A *Forbes* online poll last month showed that 69 percent of the more than 100,000 respondents played the game at work, 32 percent for more than an hour. While this survey is likely skewed, clearly workers are playing the game while on the clock.

There is an obvious productivity drag that likely comes from playing the game. However, employers are also responding to the risks of employees not paying attention to their surroundings and creating an unsafe situation at work. In addition, employers should be conscious that many workers are playing the game on phones that their employers have provided. There are liability concerns with any possible use or misuse of corporate communications tools.

Of course, some companies are looking at the craze as an opportunity and outlet for employees to bond. According to workplace wellness consultant BHS, "Pokémon Go is designed to be played by lots of people in the same area simultaneously. By chasing and catching the same monsters, users are drawn to specific locations and many people can easily connect and socialize over Pokémon. Pokémon Go has become a great bonding experiment. When your employees are meeting up around the office to discuss the game, they are doing more than just talking. They are coming together and socializing. This type of team-building interaction will help build friendship and trust between employees, which will ultimately improve morale and engagement levels in the workplace."

Coming next

September Technology@work—Unsubscribe: How e-commerce has made us immune to information

December HRIT—Cleaning out your digital closet

What do I do now? Employees behaving badly online

Be wicked smart by using search, other research tools

Should you be watching your employees' weight?

by David Micah Kaufman

The cover story discusses the ways employers are using technology to help employees improve their health. But what exactly is motivating employers to focus energy and dollars on employee wellness?

There is quite a bit of conventional wisdom that drives the efforts. First, most employers take it as a point of fact that their wellness efforts will pay off in increased employee productivity and reduced costs. Secondly, employers equate employee weight with overall health. I am not sure I buy into all of the conventional wisdom; however, I believe deeply in the potential of technology to create real positive health outcomes for workers. Technology gives employers tools to encourage positive employee behavior and actually monitor statistics that matter.

Employee wellness myth?

We take it as an article of faith that spending on employee wellness pays off. Laura Vanderkam wrote in *Fast Company* in 2014 about being intrigued by a posting on the tracker company Fitbit's website. According to Vanderkam, "One day, I wandered over to the corporate wellness section of the website, and saw an interesting statistic: Companies with worksite wellness programs experience an 8% increase in employee productivity. It sounds impressive, but this stat (attributed to a 2005 National Business Group on Health report), raised questions. Any wellness program? Any company? Productivity is tricky."

I agree. I also think the concept of "wellness" is tricky. When I was in college, I had a healthcare economics professor who said that all of us have some type of medical problem—we just need a doctor to find it. And, if that doctor could not find anything, he was sure his friend a psychiatrist could find something. Are we encouraging and/or tracking wellness?

Vanderkam found evidence that wellness programs do have some effect. She wrote, "One meta-analysis of 42 corporate wellness studies found a 25% reduction in absenteeism and sick leave, a 25% reduction in health costs, and a 32% reduction in workers' compensation and disability costs." Those statistics really are about reducing employer costs, not necessarily employee wellness or productivity.

Weighty matters

The *bulk* of the efforts of employer wellness programs are focused on reducing employees' weight. An article last year in the *American Journal of Managed Care* took a contrarian view of weight-related health efforts, concluding, "We find that most corporate weight control programs (and wellness programs generally) fail—using valid metrics, none have reported savings, long-term weight loss, or reduction in medical events over a sizable population for 2 years or more, accounting for dropouts and nonparticipants."

When we say we are trying to control weight we are really talking about fighting obesity, right?

What does obese look like?

We all assume that we know what obesity looks like. It turns out, however, that there is a standard definition of what an obese person is. It is all part of someone's body mass index (BMI). The National Institutes of Health (NIH) states, "The most common way to find out whether you're overweight or obese is to figure out your body mass index (BMI). BMI is an estimate of body fat, and it's a good gauge of your risk for diseases that occur with more body fat."

You calculate your BMI by using your height and weight (divide your weight in kilograms by the square of your height in meters {your height, multiplied by itself}). The BMI categories include:

- Underweight = <18.5;
- Normal weight = 18.5–24.9;
- Overweight = 25–29.9; and
- Obese = BMI of 30 or greater.

It is a pretty blunt measurement. Even the NIH gives 2 caveats to using BMI: (1) "It may overestimate body fat in athletes and others who have a muscular build" and (2) "It may underestimate body fat in older persons and others who have lost muscle."

David Belk, a medical doctor, assailed using the BMI on the *Huffington Post*, saying "the current BMI formula appears to assume that we're all two dimensional, as though we're cut out of cardboard."

Focus on actions and outcomes

Given the challenges of measuring weight loss, to answer the question in the title of this column, no, I don't think we should be watching the weight of our employees. Weight is just a number indicating how heavy you are. There are healthy heavy people and unhealthy light people.

Instead, use the technology we have to encourage employees to do good things. Get lots of steps (although the 10,000-step-daily goal is even more bogus than the BMI metric). Move around in the office. Do some exercise three or four days a week that significantly raises your blood pressure for 30 minutes. Eat better.

Technology can help employees do all of those things. I am not sure whether or not the activities will help reduce their BMI, but I am pretty confident that your workforce will be healthier, happier, and maybe more productive.

David Micah Kaufman is the founder of BIGGER PIES!—a boutique professional services consulting firm in San Francisco—and a regular contributor to HR Insight and HRIT. You can reach him at westward20@aol.com or 415-272-8115.