Federal Bar Association
Labor and Employment Law Section
Winter 2017

The Labouring Oar

Message from the Chair

By Corie Tarara

The Labor and Employment Section is busy as ever, and we're excited to share with you several upcoming opportunities to get involved and meet up with your colleagues. Our 7th Biennial Labor and Employment Law Conference is being held March 9-10 at the Hilton Palacio Del Rio in San Antonio, Texas. We are excited to announce our keynote speaker is EEOC Commissioner Charlotte A. Burrows. In addition to Commissioner Burrows, we have a terrific lineup of speakers from private firms across the nation, the EEOC, the US Bankruptcy Court for the Western District of Texas, the DOL Veteran's Employment and Training Service, the U.S. District Court for the Western District of Texas (Austin and San Antonio), A'viands, Noodles & Company, Potbelly Sandwich Works, Lifetouch, the U.S. Department of Justice, the NLRB and the Council on American-Islamic Relations. Simply, there is something for everyone—and a wealth of knowledge to be shared and networking connections to be made. We also have sponsorships available by contacting Heather Gaskins at hgaskins@federalbar.org and would be appreciative of those willing to sponsor this great event.

In addition to the conference, the Section continues to bring our traveling half-day CLE, "Employment Law in a Nutshell," to Chapters around the nation and had successful presentations in San Diego and Phoenix, with San Juan (January 2017) and Omaha (Feb. 17) to follow. Thank you to Brian Rochel and Phil Kitzer for continuing to organize and set up these events, and to our speakers the Hon. Betsy Chestney (Western District of Texas, San Antonio Division), and Brett Strand (3M). Further, we continue to publish the monthly Case Circuit Updates, which we hope you all enjoy the new electronic format – thank you to Judge Chestney and Caitlin Andersen for their efforts with that publication. If you'd like to contribute to the monthly update or The Labouring Oar, we encourage you to reach out to them – authors are always appreciated.

Finally, I want to thank all of the Board and Committee members for their tireless work, and believe it is because of them that our Section remains the active Section that it is. We work hard to make sure the Section continues to provide top-notch services to its members. If you'd like to get involved in any way, please reach out to me or any of the Board or Committee members. Hope to see you all in March! ■

A Look at What's Inside

The Labouring Oar is published by the Federal Bar Association Labor and Employment Law Section, 1220 N. Fillmore St., Suite 444, Arlington, VA 22201, (571) 481-9100, (571) 481-9090 (fax). ISSN 1080-1316.

Federal Bar Association

7th Biennial

LABOR & EMPLOYMENT LAW CONFERENCE

March 9–10, 2017

Hilton Palacio Del Rio • San Antonio, Texas

Join us for this two-day conference where leaders in employment and labor law from around the nation will present on timely and important topics for practitioners, including EEOC and NLRB updates, sex and sexual orientation discrimination, USERRA, immigration law, and more.

Visit www.fedbar.org/Labor17 today for more information.

Follow the FBA: | www.fedbar.org

"Game Over for the New Overtime Rule?"

By Ashleigh Leitch

Management-side labor and employment attorneys and in-house counsel spent the last six months reviewing the U.S. Department of Labor's new overtime rules, identifying which employees would be affected, and implementing the new rules by advising their clients to hire new workers, re-classify previously exempt workers, and budget for overtime expenses. However, one week before the rule became effective, a Texas federal court granted a nationwide temporary injunction blocking the rule. This article evaluates the purpose behind the overtime rule, its current status, and how to advise clients going forward.

Looking Back – What Was This Overtime Rule All About?

On May 18, 2016, the U.S. Department of Labor announced its administrative rules expanding eligibility for overtime pay to approximately 4.2 million workers under the Fair Labor Standards Act (the "FLSA"). The new overtime rule (the "Overtime Rule") proposed to significantly affect employers with exempt, salaried employees who made less than $47,476 per year.

Under the FLSA, an employee is entitled to minimum wage and overtime pay, unless she or he is "exempt" from those requirements. Under the current rules, employees are exempt from the FLSA if they meet both parts of the following test: (1) they earn a salary of at least $23,660 per year; and (2) their job duties primarily involve administrative, executive, or professional functions.

The Overtime Rule raised the salary level from $23,660 ($455 per week) to $47,476 per year ($913 per week). This presented employers with three obligations towards employees paid less than $47,476 per year: (1) pay the employee overtime pay (time and one-half) for each hour of work performed over 40 hours per work week; (2) pay the employee an hourly wage that complies with minimum wage laws; and (3) keep detailed records of the hours worked by and payments made to the employee.

The Pew Research Center estimated that the Overtime Rule would have the greatest impact on first-line managers of retail sales workers and administrative or office support staff; accountants and auditors; general, operations, and financial managers; designers; and human resource workers and managers. Teachers and some seasonal workers were excluded from the Overtime Rule.

Where Are We Now?

On November 22, 2016, Judge Amos L. Mazzant III of the U.S. District Court for the Eastern District of Texas granted a preliminary injunction in *State of Nevada, et al. v. U.S. Dep't of Labor*, No. 4:16-CV-00731. On behalf of their state employees, twenty-one states joined this emergency motion: Alabama, Arizona, Arkansas, Georgia, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Michigan, Mississippi, Nebraska, New Mexico, Nevada, Ohio, Oklahoma, South Carolina, Texas, Utah, Wisconsin. In a separate lawsuit before Judge Mazzant, fifty private business groups fully briefed a motion for summary judgment under the Administrative Procedure Act to prohibit implementation of the Overtime Rule, which is currently pending before the court. These business plaintiffs include the U.S. Chamber of Commerce, the National Association of Manufacturers, the National Retail Federation, the National Automobile Dealers Association, and the National Federation of Independent Business.

Judge Mazzant, an Obama appointee to the federal bench, granted the injunction after agreeing that the U.S. Department of Labor exceeded the authority delegated to it by Congress to interpret the scope of the salary level for executive, administrative, and professional exemptions under the FLSA. Judge Mazzant held that the Labor Department's doubling of the salary level over-emphasized that component at the expense of the job duties test, which Congress intended to be the primary test for exemption classification. Because the U.S. Supreme Court previously affirmed the Labor Department's authority to apply its salary-basis regulations in *Auer v. Robbins*, 519 U.S. 452 (1997), the injunction and its reasoning was somewhat surprising.

On December 1, 2016, the day the Overtime Rule was intended to go into effect, the Labor Department filed a notice of appeal of the order granting the preliminary injunction to the U.S. Court of Appeals for the Fifth Circuit. The Labor Department also filed a motion for an expedited briefing schedule, which the Fifth Circuit granted. However, even with the expedited schedule, President-elect Donald J. Trump will be sworn in before briefing is completed or oral argument is scheduled on the appeal. It is not clear whether the Trump Administration's Department of Labor will proceed with or withdraw the appeal.

Looking Forward—What Will Happen to the Overtime Rule?

One of the biggest unanswered questions is how the Trump Administration will handle the Obama Administration's appeal of the preliminary injunction. While on the campaign trail in August 2016, then-candidate Donald Trump did not reject the Rule in its entirety. Instead, he stated that he would "carve out" small businesses from having to comply with the Overtime Rule.

In contrast, President-elect Trump's choice for Labor Secretary has come out strongly against the Overtime Rule. Trump's nominee is Andrew Puzder, C.E.O. of CKE Restaurants, the parent company of fast food chains Carl's Jr. and Hardee's. Back in May 2016, Mr. Puzder published an opinion piece in Forbes roundly criticizing the Overtime Rule as an ineffective regulation, stating: "This new rule will simply add to the extensive regulatory maze the Obama Administration has imposed on employers, forcing many to offset increased labor expense by cutting costs elsewhere. In practice, this means reduced opportunities, bonuses, benefits, perks and promotions." If the Senate confirms Mr. Puzder as Labor Secretary, it seems highly unlikely that he would direct the Labor Department to continue litigating the appeal before the U.S. Court of Appeals for the Fifth Circuit.

On top of the Trump Administration's regulatory decisions, Congress may intervene. Well before the injunction, a bi-

partisan group of lawmakers introduced two bills: H.R. 5813 and H.R. 4773 and its companion S. 2707. These bills would stagger the increases to the salary level, and would cap the salary level at an amount lower than the that contained in the Overtime Rule. These bills are still in their very early stages but are worth watching.

Three Recommendations

In the face of so much uncertainty, how should employers proceed? Here are three recommendations.

First, if your clients have not done so already, now is the time to audit classifications to make sure that all employees have the appropriate exempt or non-exempt status. Just because the salary level test is uncertain does not mean that employers get a pass on the salary basis or job duties tests.

Second, if your clients made adjustments in anticipation of the Rule's December 1, 2016, effective date, stay the course. If the Fifth Circuit reverses the preliminary injunction, it is possible the decision could be retroactive to December 1, 2016. Reneging on a pay raise would almost certainly harm employee morale, and may invite unpaid wages and promissory estoppel claims, depending on state law.

Third, if your clients decide to take their chances by rolling back their implementation of the Overtime Rule, make sure they act uniformly. Moving forward with implementing pay raises for some but not all who would have been affected by the Overtime Rule could invite future discrimination claims. ■

Ashleigh Leitch is an attorney with Best & Flanagan in Minneapolis, where she advises employers on compliance with federal, state, and local employment laws, as well as employees on their rights in the workplace. She also defends companies in employment litigation. Ashleigh can be reached at aleitch@bestlaw.com.

L&E Section's "Traveling CLE" Set to Continue in 2017

The L&E Section is dedicated to finding new ways to give back to its growing membership. In that spirit, last year, past Chair Donna Currault and current Chair Corie Tarara introduced the traveling CLE program. The program, entitled "Employment Law in a Nutshell," was presented five times in 2016, in New Orleans, Minneapolis, Oklahoma City, San Diego, and Phoenix.

"Nutshell" is designed to educate generalists and younger lawyers interested in specializing in employment law on the issues most frequently encountered by employment practitioners, including EEO and FLSA matters as well as state-specific employment laws and regulations. Two speakers, Brett Strand and Betsy Chestney, traveled to the five cities to present the federal-law component of the program. In each city, they were joined by employment-law specialists who covered unique aspects of state and local law that affect employers and employees. Strand, who works in 3M Office of the General Counsel, was recently promoted from Senior Counsel for Employment to Senior Counsel for International Operations. Chestney has left the Austin-based employment-law boutique firm of Cornell Smith Mierl & Brutocao LLP to become a United States Magistrate Judge in San Antonio. Consequently, new national speakers are being scheduled for programs in 2017.

The next presentation is scheduled for San Juan, Puerto Rico on Feb. 4, 2017. Scheduled speakers include: Anh Le Kremer, General Counsel, Center for Diagnostic Imaging, who will cover federal employment-law compliance; Vanessa Garcia, Supervisory Attorney, NLRB, who will cover labor law; and Kathryn Gonzales-Valentin, Chair of L&E Practice, *Ferraiuoli* Law, who will cover Puerto Rico employment laws.

Phil Kitzer (kitzer@teskemicko.com) and Brian Rochel (rochel@teskemicko.com) serve as Co-Chairs of the Programming Committee and are organizing future presentations. "Nutshell" allows chapters to host a program with much less effort than is required to design a program from scratch and can be customized to your jurisdiction. If you are interested in being a traveling presenter who presents the federal-law component of the program, or if your local Chapter is interested in partnering with our L&E Section to have speakers present this program in your city, contact Kitzer or Rochel. ■

The "Nutshell" CLE was presented in Phoenix by Brett Strand, Betsy Chestney, and Ed Robaina and was organized by Andrew Breavington, President of the Phoenix Chapter.

Barbarians at the gate? Data security concerns for the employer and counsel

By Andrew J. Broadaway

If you or your clients aren't worried about it, you probably should be. *Hacking. Data breach. Data theft. Ransomware.* I know what some of you are thinking: 'Oh, come on—we employment lawyers don't need to be concerned with this too, right? We have enough on our plates keeping up with multi-state and federal employment laws. That's a job for IT departments and compliance counsel!' I'm here to remind you: not necessarily.

With the now-constant headlines reporting state-sponsored hacking, big-business data breaches resulting in the loss of millions of dollars and consumer trust, and individuals' and businesses' vital data being hijacked and held for ransom, you would be forgiven for thinking maybe you and your clients should go back to keeping paper files and corresponding via carrier pigeon. With all of this bad news, data security experts' oft-quoted maxim now seems truer than ever—it's not a matter of "if" you or your clients will suffer some sort of data incident, but "when." At the risk of sounding alarmist, the past several years have shown such incidents occurring, or at least being discovered, at an ever-increasing rate. And, despite promises of our fully digital future, there appears to be no ultimate technical solution in sight. This all suggests that data security and breach response will be responsible for driving up business costs, legal expenditures, and IT budgets for the foreseeable future.

Of course, many of you are already aware of the risks involved with our Internet-connected world. And many of you have sophisticated clients with technological and administrative safeguards in place to manage their risks. Maybe some of your clients have robust incident-response plans and have consulted with advisors trained in preventing and dealing with data incidents. Perhaps even some of your clients have weathered such incidents, with or without your guidance. However, I am certain that some of you represent small-to-medium employers who feel like they do not face much risk from cyber threats. Therefore, they cannot justify the expense of addressing those supposedly distant risks. Or maybe you represent a company that, correctly, believes it does not deal in "data" in the traditional sense. Because the client does not process payments or deal directly with consumers' information, it feels unlikely to be the target of a cyber-attack or at risk for a data incident.

Employers Face Significant Data Risks Too, Even If The Business Is Not Data-Centric

Quick poll: how many of your clients' businesses are not connected to the Internet? OK. Now, how many of your clients' employees never access company computer systems in any way? If you raised your hand both times, you can probably stop reading. For the rest of you, it is important to counsel your clients regarding this basic truth: employee data, meaning data the employer collects and maintains about its own employees, is constantly at risk of breach and disclosure, from both external and internal sources. That's right. A disgruntled employee can do even more damage than an external hacker, given that person's knowledge of your systems. Disclosure of employee information, regardless of its source, carries legal risk similar to, if not worse than, the breach of customer data. The data an employer collects about its employees is necessarily the most personal in nature. HR departments maintain files that might include health information, financial account information, social security numbers, driver's license numbers, tax information, and addresses. Moreover, the company likely has at least some of that information on an employee's spouse or children.

All of that private information is like gold to hackers and criminals, and it is equally sought after. And, if disclosed, employee data can have more serious long-term impact that a stolen credit card or PIN number. Whereas fraudulent charges can often be quickly remedied by a card issuer, identity theft lasts forever (or at least feels like it). Therefore, if employee data is handled improperly or is inadequately safeguarded, or if that data is disclosed or stolen, an employer could have big problems. Moreover, if the breach, once discovered, is not handled in compliance with state—and even international—laws, the problems could be magnified. At worst, employees could bring a class-action lawsuit and employers could be on the hook for penalties, damages, and public notoriety—and not the good kind.

A Recent Example Of Employee Data Breach Resulting In Litigation

That appears to be the situation Sprouts Farmers Market is facing in a recently filed series of lawsuits. The cases, now consolidated and pending before U.S. District Judge Douglas Rayes in the District of Arizona *(see IN RE: Sprouts Farmers Market Incorporated Employee Data Security Breach Litigation,* 2:16-md-02731), feature current and former employees of Sprouts who allege that their personal identifying information ("PII") was accessed, stolen, and used without their authorization. The proposed class consists of more than 21,000 employees who are alleged to have had their full names, addresses, social security numbers, wages, and tax withholdings improperly disclosed. Plaintiffs allege that a Sprouts employee emailed unencrypted W-2 statements for all employees to an unknown person. The disclosing employee is alleged to have fallen victim to a phishing scam, believing that he or she was responding to a legitimate email request from a Sprouts executive. Further allegations detail a litany of horribles resulting from the disclosure of the PII: identity theft, credit reporting problems, tax fraud and refund theft, medical fraud, and, of course, resulting economic and noneconomic damages. The lawsuits allege that Sprouts failed to abide by the breach notification laws of most states, including California and Arizona. Additionally, Sprouts stands accused of acting negligently for how the company stored and maintained its employee records and how it disclosed the W-2 forms.

Regardless of the outcome of this particular or other, similar litigation, one message is clear: the risk to employers is real, and the consequences are costly. It is easy to look at cases like *Sprouts* and think 'Wow, that's bad, but it would never happen to me or my client.' Assuredly, basic safeguards like encrypting and password-protecting sensitive data might have helped prevent the particular outcome for Sprouts. As might security-awareness training for employees or robust email-filtering tech-

nology to block phishing attempts in the first place. Companies of all sizes should definitely devote appropriate resources to preventive measures, both technological and administrative. However, no amount of technology or training will prevent all incidents. The criminals are almost always innovating ahead of the technological curve, and training relies on imperfect people always remembering to be perfect.

At a recent CLE event an experienced attorney, savvy with computers and versed in current threats, detailed how he fell victim to a ransomware attack. He was busy and distracted, receiving dozens of legitimate emails that afternoon with attachments. The email in question appeared to be from someone he knew, and he was expecting an email from that sender. He clicked on the attachment instinctively and then realized, almost instantly, that it wasn't a real attachment but, instead, was a program. The software had started encrypting his files, starting with the most recent ones. After a few seconds of flailing, he had the presence of mind to unplug the computer's power cable and take the hard drive to a forensic specialist for recovery. He was lucky—he lost only a couple of weeks of work, and he did not have to pay a hacker to get years of his work product back. The point of that story, other than serving to scare me into triple checking every attachment, was that, no matter how careful you are or how much your clients trust their security systems, all it takes is a momentary lapse to suffer a data incident with lasting consequences.

What Are Employers And Their Counsel To Do?

The most important piece of advice? Have a plan. Often called an "incident-response plan," companies (and the law firms that support them) should have a written, researched, communicated, and practiced plan in place well before any incident occurs. The plan can be simple or elaborate, depending upon the complexity of the organization and the amount and type of data that it keeps. Each employer's plan should start by cataloging all types of sensitive data maintained by the organization, who uses it, who has access to it, how it is stored, where copies of such data might exist, and the safeguards in place to protect it.

Identify Your Response Teams

A response plan should also designate internal and external crisis teams. Internal teams should be small, agile, and well trained—familiar with the IT systems and data in question. They should also include, or at least directly report to, senior management. Keeping the initial stages of incident investigation and response absolutely confidential is critical; sometimes incidents are not as serious as they initially appear, and unsubstantiated or false rumors of a data breach can be extremely damaging to company morale and reputation.

External teams should likely include counsel or someone well-versed in privacy and breach reporting, assuming those are not resident in-house. In addition, companies should consider ongoing relationships with crisis-management and forensics vendors as part of their plan. Vendor contracts should be signed well in advance of any incident, and the team dynamics and professional relationships should be well-established. There is nothing worse than having to scramble to review vendor contracts and coordinate unknown personnel while the breach-notification timeline is ticking down, or even worse, if the breach is still actively happening.

Flexibility Is Key

Another vital thing to remember: make sure your plan is flexible enough to deal with small incidents, as well as large ones. Most companies' incident-response plans seem to focus almost exclusively on catastrophic data breach—the ones that make the headlines. Certainly, large-scale hacks originating from outside the company do happen. Just ask Sprouts, the U.S. Office of Personnel Management, and SnapChat, to name a few. However, more realistic, and more frequent, are smaller-scale internal incidents. You get a report that one of your client's HR generalists has lost a thumb drive containing a spreadsheet compiling sensitive employee data. The plan should cover that. A review of a recently terminated employee's computer activity shows that he was emailing himself attachments suspected to contain protected data. Your plan should cover that too.

Practice and Communicate

Almost as important as having a plan is practicing the plan. This may involve something as simple as tabletop strategy sessions going over the aspects of the plan with all key personnel. Or it could involve a full-scale simulated incident where only very few of the players know that it is a drill. Nothing will identify shortcomings in an incident-response plan quite like a realistic simulation. Often, executing certain aspects of a data-incident response are time-critical. Identifying bottlenecks or missing communication channels before there is an actual event can sometimes mean the difference between timely remediation or blown breach-notification deadlines.

It may seem obvious, but a crucial precursor to practicing the plan is making sure that it is well documented and communicated to crucial team members, including their backups. But equally vital is making sure that rank and file personnel are aware that an incident plan exists and that they know to report an incident when it happens. Returning to the lost HR thumb drive example: if the HR generalist is not aware that he needs to report the loss of sensitive HR data, it might go unnoticed until too late. If the HR generalist reports the loss to his manager, but the manager does not report the incident up the chain to activate the incident-response protocol, the company may have suffered a report-triggering breach, but failed to timely act and notify necessary parties.

Revisit, Revise, Repeat

Finally, incident-response plans are not intended to be static documents. Changes in management, personnel, reporting, IT infrastructure, vendors, or HR practices may all trigger a need to revisit and revise the plan. New attack vectors or technological vulnerabilities may be discovered that require a different approach to your incident response. Also, as will be discussed below, your jurisdiction's breach notification laws may change, rendering certain aspects of your plan obsolete. Make sure that your client knows that they should be revisiting their incident-response plan with regularity, optimally in conjunction with a practice run or whenever the

company undergoes significant operational changes.

Breach Notification for Employers

A full discussion of data breach notification laws and how they differ between various states and countries is far beyond the scope of this article. But as the *Sprouts* cases demonstrate, incomplete or untimely compliance with applicable state notification laws can be a major source of liability. The challenges facing multi-state or multi-national employers are legion. There is no uniform approach to notification triggers, which information is required to be disclosed to affected parties, when state entities must be informed, and the timing of notification after the disclosure is discovered. Generally speaking, the United States lags behind the rest of the world when it comes to privacy regulation, so if you are advising clients with international employees, they should be prepared to comply with much stricter rules.

Expanding State Laws

Forty-seven states (all but Alabama, New Mexico, and South Dakota), the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring private entities to notify affected individuals of security breaches involving their personally identifiable information. The legislation differs, but nearly all have provisions defining who must comply with the law, what constitutes personal information, what constitutes a breach, the requirements and timing of notice, and exemptions to the notification requirements. Recent trends show that states are amending their breach notification requirements to be broader, and require more and earlier notification. Eight states amended their breach notification laws in 2015 to add new and unique requirements. In 2016, at least 26 states have introduced or are considering security breach notification bills or resolutions, mostly amending existing legislation to expand coverage.

Inconsistencies between existing state laws and staying on top of constant amendments can create compliance nightmares for multi-state employers. For example, in October 2015, California amended its breach notification law and mandated a specific form of notice with required information and specific headings. However, other states may require different, or additional, information to be shared. Massachusetts and Rhode Island mandate that affected individuals be informed of their right to obtain a police report, but California does not. Wyoming requires that a breach disclosure specify whether law enforcement requested the affected entity to delay notification. This inconsistent approach renders a single notice form almost impossible to draft.

Know Your Triggers

Knowing what events "trigger" breach notification laws is also vital. Different categories of information may be treated differently in neighboring jurisdictions. What is considered PII in one state may not be in an adjacent state. However, as a general rule, names and associated SSN's will nearly always trigger a breach law. Also, the size of the breach and the affected number of employees may trigger different reporting requirements. Nearly half of states require reporting data breaches to the state's Attorney General; many of those mandate such disclosure regardless of the number of individuals affected. Other states require notice to state regulatory bodies or investigative entities. State involvement can lead to administrative inquires and possible fines.

Don't Delay Once You Learn Of An Incident

Breach notification deadlines are another source of inconsistency and confusion. While most states' laws provide a flexible notification deadline, typically "as soon as reasonably practicable" or "without unreasonable delay," that's not always the case. Some states already impose strict deadlines, and other states appear to be following suit. Ohio, Rhode Island, Tennessee, Vermont, Washington, and Wisconsin require notice to be delivered within 45 days of the discovery of the breach. Florida requires notice within 30 days. These deadlines are a critical part of any employer's incident-response plan, and the importance of complying with the deadlines cannot be understated.

Keep Calm And Carry On

As sobering as it is to realize the risks facing most of our clients by virtue of the sensitive employee data they all maintain, take a deep breath. All is not gloom, doom, and litigation headaches. If you and your clients plan for—and execute—appropriate protection measures and calculated responses, the inevitable data incident can be dispatched with minimal disruption to normal business. Nearly every employer faces some risk of a data breach; our HR departments could not function without collected data. However, the consequences of an incident are exacerbated by responding inappropriately or, worse, not at all. With these topics in mind, you should be able to help your clients plan for risks that some may not have even known existed.

Luckily for all of us, there are many free or inexpensive resources available to help the employer and their counsel navigate this complicated environment. Employers should also check with their insurance providers, as many are now offering policies to help offset the cost of an incident. If you or your clients face a data incident before having developed and refined a response plan, don't panic. While it is probably wise to consult with counsel familiar with breach and incident response and who can guide you in remediation, you will not be alone in dealing with these challenges. ■

Andrew J. Broadaway is an attorney specializing in labor and employment litigation and employer counseling with the Austin, Texas law firm Cornell Smith Mierl & Brutocao, LLP. He is also a Certified Information Systems Security Professional (CISSP #322890) and member of the International Association of Privacy Professionals. Andrew's previous career as an information security consultant gives him a unique perspective on the data security and privacy issues facing employers. Andrew can be reached at: abroadaway@cornellsmith.com.

A Membership Perk: Monthly Circuit Updates

Don't forget that your membership in the Labor and Employment Section gives you access to the Monthly Circuit Updates! Each month, summaries of all the major labor and employment decisions in each Circuit are provided to all members in an eNewsletter that is also available on the Section's webpage at www.fedbar.org/sections/labor-employment-law-section.aspx. These Updates are an invaluable resource that allows members to stay up-to-date on important developments in each Circuit. Take a deep dive into all the new cases within your Circuit each month, and/or peruse all of the developments around the country to stay abreast of the law for your clients. If you would like to volunteer as a contributor for the Circuit Update, please contact Caitlin Andersen (candersen@seatonlaw.com) or Betsy Chestney (bchestney@cornellsmith.com) for more information.

2016 OSHA Overview

By Dana Swanson

2016 saw a whirlwind of new regulations from the Occupational Safety and Hazard Administration (OSHA), changes that enhance penalties, establish electronic data submission for injuries and illnesses, and affect the requirements relating to silica exposure, eye/face protection, and walking-working surfaces. This article outlines OSHA's new rules, some of which have already taken effect. Given President Donald Trump's advocacy of "a requirement that for every new federal regulation, two existing regulations must be eliminated," it will be interesting to see how federal workplace restrictions evolve during 2017.

Penalties for OSHA Violations Increase

New maximum penalties for OSHA violations went into effect on August 2, 2016, raising the maximum potential penalties for employers by 78 percent. Any violations that occur on or after August 2, 2016 are subject to the increased maximum penalty rates. The last update to OSHA's penalty fees occurred in 1990, and according to OSHA the 2016 increase adjusts for inflation over the past 26 years. Penalties will also increase every year on January 15 based on annual cost-of-living.

Serious violations were previously subject to a $7,000 penalty per violation, however, as of August 2, 2016 these violations may incur up to a $12,471 penalty. Penalties for failures to correct a violation after an issued citation rose from $7,000 per day beyond the abatement date to $12,471 per day beyond the abatement date. Willful or repeated violation penalties rose from $70,000 per violation to $124,709 per violation.

States operating their own safety and health programs must adopt maximum penalty levels that are at least as effective as OSHA's maximum penalties.

Final Rule for Electronic Submission of Injury and Illness Data

On December 19, 2016, OSHA finalized a rule requiring certain employers to electronically submit injury and illness data already collected by employers. 29 CFR §§ 1902, 1904. The rule goes into effect January 1, 2017, and the information submitted by employers will then be publicly posted on a new website. This publicly posted content will not contain employees' personally identifiable information (e.g., employee name, address, name of physician, etc.). However, information identifying the employer will not be redacted. OSHA claims the rule will be instrumental in "nudging" employers to focus on safety and discourage retaliation against employees for reporting injuries and illnesses.

Employers with 250 or more employees must electronically submit injury and illness information to OSHA via OSHA Forms 300A (Summary of Work-Related Injuries and Illnesses) beginning July 1, 2017, and Form 300 (Log of Work-Related Injuries and Illnesses) and 301 (Injury and Illness Incident Report) beginning July 1, 2018. Employers with 20–249 employees in "hazardous" industries must electronically submit information from Form 300A beginning July 2017. "Hazardous" industries under the new requirements include: construction, taxi service, vending machine operators, nursing homes, grocery stores, and agriculture.

States with safety and health programs must adopt requirements that are substantially identical to the new OSHA approach within six months after the publication of the final rule.

The final rule also requires that employers' policies and procedures for reporting work-related injuries and illnesses should not deter or discourage a reasonable employee from accurately reporting or allow for any retaliation from reporting an injury or illness. Employers should make sure they have the mandatory OSHA workplace poster, informing employees of their right to report work-related injuries and illnesses without retaliation.

Although the new rule does not strictly prohibit post-accident drug testing of employees, employers are prohibited "from using drug testing, or the threat of drug testing, as a form of retaliation against employees who report injuries or illnesses." Employers should examine their workplace safety incentive programs and drug testing programs to ensure they are not "blanket" policies, likely to be scrutinized by OSHA as being retaliatory or deterring injury or illness reports. The new rule does not add any additional obligation to complete, retain, and certify injury or illness records.

Final Rule for Permissible Exposure to Silica

On March 24, 2016, OSHA issued a final rule reducing the permissible exposure limit for respirable crystalline silica. 29 CFR §§ 1910, 1915, 1926. The new requirement reduces the permissible exposure limit from 100 micrograms to 50 micrograms per cubic meter of air in an 8-hour shift. Under the final rule, employers are required to use engineering controls to limit worker exposure (OSHA offers water or ventilation as examples of possible engineering controls), provide respirators (when exposure limits are not adequately limited by engineering controls), limit worker access to high exposure areas, develop a written plan to limit exposure, offer medical exams to workers who work in high exposure areas, and train workers on the potential risks of silica exposure and how to limit exposure.

The final rule went into effect on June 23, 2016, however some industries have up to five years to comply with the requirements. The construction industry must comply by June 23, 2017. General industry and the maritime industry must comply by June 23, 2018. The hydraulic fracturing industry must comply by June 23, 2018 (with the exception of the engineering controls industry, which must comply by June 23, 2021).

Final Rule for Eye and Face Protection Standards

OSHA issued a final rule updating its standards for workers' personal protective equipment in general industry, shipyards, longshoring, marine terminals, and construction. 29 CFR §§ 1910, 1915, 1917, 1918, 1926. This rule went into effect on April 25, 2016. According to OSHA "[t]he final rule reflects current national consensus standards, and ensures that workers can use up-to-date eye and face protection."

The new rule replaces the outdated 1986 edition of the national consensus standard on eye and face protection with criteria approved by the American National Standards Institute (ANSI) and published by the International Safety Equipment Association (ISEA). The new standard sets forth the design, performance specifications, and markings of products used to protect the eyes and face. The construction industry standard was similarly amended, removing the 1968 ANSI standard while implementing the above referenced standard.

Although OSHA requires that employers make sure their employees use eye and face protection when necessary, the new rule does not require the replacement or updating of protective equipment. Employers may continue to follow their usual practices for face and eye protection and should use the updated rule as a national industry standard guideline when selecting eye and face protection.

Final Rule for Walking-Working Surfaces Standards

On November 17, 2016, OSHA finalized its rule on Walking-Working Surfaces and Personal Fall Protection Standards. 29 CFR § 1910 subpart D and I. The new rule amends and adds language regarding ladders, rope descent systems, and fall protection systems and goes into effect on January 17, 2017. OSHA anticipates that the changes provided under the new rule will prevent 29 fatalities and 5,842 lost-workday injuries annually. Most provisions went into effect on January 17, while other provisions are delayed. For example, employers have six months to train their workers on fall hazards and equipment covered under the rule, giving employers time to devise and implement training plans. Additional compliance dates for various portions of the new rule extend to 2036.

The previous regulations required employers to use guardrails to protect workers from potential falls, whereas the new OSHA rule grants employers some flexibility in selecting a personal fall protection system that works best for their environment. OSHA believes this flexibility will allow employers to determine what structure will be most effective in the employer's individualized workplace to best protect their employees.

In addition, the rule permits employers to use Rope Descent Systems (RDS)[1] so long as the RDS is not being used at heights above 300 feet. The OSHA rule requires building owners to inform employers, before a RDS is used, that the permanent RDS anchorages have been identified, tested, certified, and maintained. This information must be based on an annual inspection and each anchorage must be certified at least every 10 years (or earlier when necessary). Among other requirements, employers must not allow any employee to use an RDS system without having obtained written information from the building owner that each anchorage meets the above requirements, the RDS is used in accordance with the manufacturer's instructions, warnings, and design limitations, the RDS has been inspected before each workshift, and the employees are trained on the RDS.

The new rule also provides specific regulations about ladders, including that ladders must be able to support their maximum intent load, and that ladder stands and platforms must be able to support four times their maximum load.

In addition, employers must train employees on the nature of the fall hazards in the work area and how to recognize them; the procedures to be followed to minimize those hazards, the correct procedures for installing, inspecting, operating, maintaining, and disassembling the personal fall protection systems that the employee uses; and the correct usage of the personal protection systems and equipment. ■

Dana Swanson is a 3L at the University of Minnesota Law School. She is currently a law clerk for Seaton, Peters, & Revnew in Minneapolis, MN.

Endnotes

[1]RDS is a suspension technique that allows workers to descend and stop in a controlled manner in order perform work at greater heights. While this system is allowed under OSHA, some states' regulations differ on height limitations and whether RDS should be allowable at all.

NEW MEMBERS

The Labor and Employment Section welcomes its new members:

Clifford S. Anderson
Matthew Paul Bachochin
Jennifer E. Bowen
Mitchell Calhoun
Megan J. Crowhurst
Craig Curwood
Lauren Elizabeth Fisher White
Michael A. Foley
Stanley R. Foreman
Alanna Francois
Jason Friedman
Harold Anthony Frye Maldonado
Amber Helena-Therese Gardina-Quintanilla
Ryan Keith Geddie
Janna M. Giesbrecht-McKee
David G. Greco
Mary C. Hamm
Michael P. Kelly
Nadia A. Klarr
Roy Richard Love
Christie Marie Merchant
Arrissa Kathryn Meyer
Krysta Marie Mitchell
Pablo Orozco
Brad Gary Pelc
Daniel Riegel
Cynthia Rios
Samuel Sadeghi
T. Thomas Singer
Frank Totti
Matthew Aaron Tripp
Faith Clair Whittaker
Keith Andrew Wilkes
Ryan Adam Winters
S. Wesley Woolf
Mitchell Aaron Wrosch

We encourage each of you to become involved in Section activities. Consider joining us for the section's 2017 Bienniel Conference in San Antonio, March 9-10. Also, visit our webpage (www.fedbar.org/sections/labor-employment-law-section.aspx) to take advantage of the information and resources available there, and watch for our monthly Circuit Updates to stay abreast of recent developments in labor and employment law.

Again, welcome! We look forward to counting you among the ranks of our active members.

Labor and Employment Law Section Governing Board

CHAIR
Corie Tarara
Seaton, Peters & Revnew, P.A.
7300 Metro Blvd. Suite 500
Minneapolis, MN 55439
(952) 921-4615
ctarara@seatonlaw.com

VICE CHAIR
Kathryn M. Knight
Stone, Pigman, Walther, Wittmann LLC
546 Carondelet St.
New Orleans, LA 70130
(504) 593-0915
kknight@stonepigman.com

DEPUTY CHAIR
Craig A. Cowart
Jackson Lewis P.C.
999 Shady Grove Road
Suite 110
Memphis, TN 38120
(901) 462-2618
craig.cowart@jacksonlewis.com

SECRETARY
Elizabeth "Betsy" Siberry Chestney
U.S. District Court
John H. Wood, Jr. U.S. Courthouse
655 East Cesar E. Chavez Boulevard
4th Floor—Courtroom B
San Antonio, TX 78206
(210) 472-6350

TREASURER
M. Kathleen McKinney
National Labor Relations Board
600 South Maestri Place
7th Floor
New Orleans, LA 70130
(504) 589-6374
Kathleen.mckinney@nlrb.gov

IMMEDIATE PAST CHAIR
Donna P. Currault
Gordon, Arata, McCollam, Duplantis & Eagan, LLC
201 St. Charles Ave. 40th Floor
New Orleans, Louisiana 70170
(504) 582-1111
DCurrault@gordonarata.com

EDITOR, *THE LABOURING OAR*
Elizabeth "Betsy" Siberry Chestney
U.S. District Court
John H. Wood, Jr. U.S. Courthouse
655 East Cesar E. Chavez Boulevard
4th Floor—Courtroom B
San Antonio, TX 78206
(210) 472-6350

STANDING COMMITTEES:
(All Chairs/Co-Chairs are members of the Governing Board)

Standing Committee on Membership and Chapter Relations:
Co-Chairs:
Craig A. Cowart
Jackson Lewis P.C.
999 Shady Grove Road
Suite 110
Memphis, TN 38120
Phone: (901) 462-2618
craig.cowart@jacksonlewis.com

Whitney Sedwick Meister
Best Western International, Inc.
6201 N. 24th Parkway
Phoenix, AZ 85016
whitney.meister@bestwestern.com

Standing Committee on Publications and Public Relations:
Co-Chairs:

EDITOR, THE LABOURING OAR
Elizabeth "Betsy" Siberry Chestney
U.S. District Court
John H. Wood, Jr. U.S. Courthouse
655 East Cesar E. Chavez Boulevard
4th Floor—Courtroom B
San Antonio, TX 78206
(210) 472-6350

Caitlin Andersen
Seaton Peters & Revnew PA
7300 Metro Blvd Ste 500
Minneapolis, MN 55439
(952) 896-1700
candersen@seatonlaw.com

Standing Committee on Programming and Continuing Legal Education:
Co-Chairs:
Brian Rochel
Teske Micko Katz Kitzer & Rochel
222 S 9th St Ste 4050
Minneapolis, MN 55402
(612) 746-1558
rochel@teskemicko.com

Phillip Kitzer
Teske Micko Katz Kitzer & Rochel
222 S 9th St Ste 4050
Minneapolis, MN 55402
(612) 746-1558
kitzer@teskemicko.com

Standing Committee on Finance and Expenditures:
Co-Chairs:
M. Kathleen McKinney
National Labor Relations Board
600 South Maestri Place
7th Floor
New Orleans, LA 70130
(504) 589-6374
Kathleen.mckinney@nlrb.gov

Karleen Green
Karleen.Green@phelps.com

Standing Committee on Executive Agency Outreach:
Co-Chairs:
M. Kathleen McKinney
National Labor Relations Board
600 South Maestri Place
7th Floor
New Orleans, LA 70130
(504) 589-6374
Kathleen.mckinney@nlrb.gov

Danielle Brewer Jones
The Brewer Law Office, PLLC
1891 Pass Rd.
Biloxi, MS 39531
(228) 388-0053
dbrewer@brewerlegalservices.com

Standing Committee on Legislation and Congressional Relations:
Co-Chairs:
Jennifer McNamara
Baker, Donelson, Bearmand, Caldwell & Berkowitz
201 St Charles Ave Ste 3600
New Orleans, LA 70170
(504) 566-5240
jmcnamara@bakerdonelson.com

Joel P. Schroeder
Best & Flanagan LLP
60 South Sixth Street, Suite 2700
Minneapolis, MN 55402
(612) 339-7121
jschroeder@bestlaw.com

Special Committee on Awards/ Marketing:
Donna P. Currault
Gordon, Arata, McCollam, Duplantis & Eagan, LLC
201 St. Charles Ave. 40th Floor
New Orleans, Louisiana 70170
(504) 582-1111
DCurrault@gordonarata.com

Special Committee on Community Outreach & Civics Education:
Joyce Kitchens
Kitchens New Cleghorn LLC
2973 Hardman Ct.
Atlanta, GA 30305
(678) 244-2880
joyce.kitchens@knclawfirm.com

CHAPTER REPRESENTATIVES:
(All are members of the Governing Board and of Standing Committee on Membership and Chapter Relations)

Timothy Bliss
CenterPlace
50 Park Row West, Suite 109
Providence, RI 02903
(401) 274-2100
TBLISSLAW@gmail.com

José Gonzalez-Nogueras
Jimenez Graffam & Lausell
Midtown Bldg. Fourth Floor
420 Ponce de Leon Ave.
San Juan, Puerto Rico 00918-3405
Phone: (787) 767-1030
Fax: (787) 751-4068
jgonzalez@jgl.com

Jim Hammerschmmidt
The Law Firm of Paley Rothman, Attorneys at Law
4800 Hampden Ln 4th Floor
Bethesda, MD 20814
(301) 951-9338
jrh@paleyrothman.com

Whitney Sedwick Meister
Best Western International, Inc
6201 N. 24th Parkway
Phoenix, AZ 85016
whitney.meister@bestwestern.com

Joyce Kitchens
Kitchens New Cleghorn LLC
2973 Hardman Ct.
Atlanta, GA 30305
(678) 244-2880
joyce.kitchens@knclawfirm.com

The Labouring Oar

Labor and Employment Section
Federal Bar Association
1220 North Fillmore Street
Suite 444
Arlington, VA 22201