



# HUMAN RESOURCES UPDATE

VOL 7, ISSUE 3

## NEW MINIMUM WAGE LAW

President Bush signed a minimum wage increase into law May 25 as part of an Iraq supplemental spending bill. Although the U.S. Department of Labor has yet to put out an official date, labor law professionals are advising that July 24, 2007 (60 days after the President's signature) will be the official date of the first of three 70-cent step increases. Based on this date, here is the schedule we anticipate for the increases:

July 24, 2007 - \$5.85

New posters should be available soon at

July 24, 2008 - \$6.55

<http://www.dol.gov/esa/regs/compliance/posters/flsa.htm>

July 24, 2009 - \$7.25

Restaurants received industry-specific tax relief in the form of a permanent FICA tax credit and related AMT relief, adding up to \$1 billion in restaurant tax relief. The overall \$4.9 billion tax package also included an extension of the Work Opportunity Tax Credit and expanded Sec. 179 expensing for small businesses. Please speak with your company's accounting firm for additional information.

## TRAINING: THERE IS TIME

A recent article in Daily Advisor discussed the similarities in answers between two groups of attorneys who were polled about key HR problem areas. The topics they agreed upon included wage and hour violations, illegal hiring practices, poorly handled leave requests, and inadequate response to harassment and discrimination charges as the most likely areas where employers get into legal trouble.

They also agreed that one necessary element to stay out of this kind of trouble is proper training of managers and supervisors. This is typically because supervisory people may know their main job functions, be it software development or accounting, but know very little about HR.

The danger is that "they don't know what they don't know" and then act on that lack of knowledge by improperly classifying workers under FLSA, asking illegal interview questions, denying protected leave, or not paying a terminated employee timely. All this may lead to a disgruntled employee.

Even brief, regularly scheduled sessions can produce outstanding results while reducing risks.

## JOB LISTING OBLIGATIONS FOR FEDERAL CONTRACTORS

The OFCCP has not yet issued its final rule concerning job listing obligations for federal contractors, although America's Job Bank closes down on June 30. The Agency has, however, issued interim guidance. In an announcement published by the OFCCP just days ago, the Agency stated that it will *not* cite contractors during compliance evaluations for a violation of the OFCCP regulations solely for their failure to list employment openings as required by the Jobs for Veterans Act (JVA).

While the OFCCP offers this temporary relief in light of the discontinuation of the AJB, the Agency specifically states that it is not releasing contractors from their obligation to pursue good faith efforts to recruit qualified veterans for available positions. The Agency reminds contractors that the listing requirement is an essential element of a contractor's good faith efforts to take affirmative action for veterans. It further says that contractors should list employment opportunities for each of its facilities with the local office of the state employment security agency wherever possible while waiting for OFCCP final guidance.

THE HOPKINS  
GROUP, LLC IS  
REGISTERED WITH  
THE NCTRCA AS A  
WOMAN OWNED  
BUSINESS AND WITH  
THE STATE OF TEXAS  
AS AN HISTORICALLY  
UNDERUTILIZED  
BUSINESS.



**THE DEPARTMENT OF LABOR IS IN THE PROCESS OF REVIEWING THE PROVISIONS OF THE FAMILY MEDICAL LEAVE ACT (FMLA), SO STAY TUNED.**

This newsletter is a periodic publication of The Hopkins Group, LLC and should not be construed as legal advice or legal opinion on any specific facts or circumstances. The contents are intended for general information purposes only and you are urged to consult a lawyer concerning your own situation and any specific legal questions you may have. For further information about these contents, please contact any representative of The Hopkins Group, LLC.

**HUMAN RESOURCES  
BUSINESS SOLUTIONS**

**THE HOPKINS GROUP, LLC  
214-597-2444  
WWW.HOPKINSHR.COM**

**COPYRIGHT © 2007  
THE HOPKINS GROUP, LLC  
ALL RIGHTS RESERVED**

## **SHRED IT OR DREAD IT**

If your business is not in compliance with various Texas Anti-Identity Theft statutes, you might receive an unwanted visit from the Attorney General. Since identity theft has become one of the fastest growing crimes, both Federal and state authorities are devoting more resources to combat and prevent identity theft. As evidenced by recent lawsuits against Texas businesses, Texas Attorney General Gregg Abbott has been aggressively pursuing violations of Texas laws designed to prevent identity theft.

Every business operating in Texas should be aware of the 2005 Identity Theft Enforcement and Protection Act ("ITEPA") and Chapter 35 of the Business and Commerce Code ("Chapter 35") each of which contain penalties for failing to properly handle certain personal information. Both laws require that an individual's sensitive personal information be protected and safeguarded with reasonable procedures to prevent unlawful disclosure and that the records containing that information be destroyed by shredding, erasing or making the record undecipherable. Failure to comply with these provisions can expose your business to penalties of \$500 - \$50,000 per violation. Additionally, a violation of these statutes might also result in a violation of the Texas Deceptive Trade Practices Act.

As Radio Shack, CVS, and other businesses who have been targeted by the Attorney General are aware, violations of these laws can result in large fines. However, that is not all. A business may also receive negative press, lose employees and customers, and be sued by employees and customers whose personal information has been compromised. The following are some steps your business can take to protect itself from exposure to enforcement.

### **Know and Understand What the Law Requires for Handling and Disposing of Personal Information**

In order to protect your company, know where originals and copies of business records containing personal information - whether in paper or electronic form - are maintained and how they are disposed. You will probably learn something you did not know about your company and its data. The types of records which must be protected under these statutes include original or reproductions of handwritten, typed, or electronically stored documents or data that contain an individual's name, social security number, driver's license number, debit or credit card number or other personal information.

Secondly, determine whether your company's processes for destroying these records comply with Texas law. The law requires that after the applicable retention period, business records are to be destroyed by shredding, erasing or making the personal information undecipherable.

Thirdly, determine if your company's processes are in writing and contained in a document/data retention and disposal policy. While not specifically required by the law, having written instructions that outline your company's legally compliant retention and disposal policies will increase awareness among your employees and help ensure full compliance.

### **Ensure Legal Compliance Procedures are in Place to Deal with Security Lapses**

Analyze and determine if your company has in place procedures for dealing with a security lapse that may disclose your customers' personal information to identity thieves. For instance, ITEPA has specific notification requirements that must be employed if a breach occurs. If there is a breach, your company must move "as quickly as possible" to notify (a) each Texas resident whose information was disclosed without authorization, (b) the owner or license holder of the data, and (c) if more than ten thousand individuals were exposed in the breach, then all consumer reporting agencies.

Many of the steps required by these laws take a common sense approach to handling and destroying business records that contain personal information. That being said, the recent push by the Attorney General's office has identified a number of large national companies that have exposed their customer's confidential information and, consequently, may be subjected to massive fines and the potential for costly litigation. In this time of increased focus on identity theft and the security of personal information, it may be time for your business to revisit its procedures for handling its employees and customers' personal information.

*Courtesy of Strasburger & Price, LLP, Strasburger Business & Law News, June 29, 2007*