

# HR Brief

Human Resources tips brought to you by  
**Baldwin Krystyn Sherman Partners**

September 2015

## DOL Clarifies Worker Classification

On July 15, 2015, the U.S. Department of Labor (DOL) issued an [administrative interpretation](#) clarifying how an employer determines whether a worker is an employee or an independent contractor.

The DOL has expressed growing concern over employee misclassification since it can have a direct impact on employee eligibility for benefits, legal protections (such as minimum wage and overtime) and taxation.

Although several tests exist for determining whether to classify a worker as an employee or independent contractor, the DOL has traditionally favored the economic realities test. This test seeks to determine whether a worker is economically dependent on his or her employer or whether the worker is in business for him- or herself. The DOL's position is that if a worker is economically dependent on the employer, the worker should be classified as an employee and entitled to all the legal protections associated with being an employee.



**BALDWIN**  
KRISTYN SHERMAN

The DOL outlines six factors for employers to consider when applying the economic realities test:

1. Is the work an integral part of the employer's business?
2. Does the worker's managerial skill affect the worker's opportunity for profit or loss?
3. How does the worker's relative investment compare to the employer's investment?
4. Does the work performed require special skill and initiative?
5. Is the relationship between the worker and the employer permanent or indefinite?
6. What is the nature and degree of the employer's control?

In its administrative interpretation, the DOL emphasized that no one factor is determinative, and the factors should not be applied in a mechanical fashion. The DOL encourages employers to use the six-factor test as a guide within the context of the Fair Labor Standard Act's (FLSA) definition of employment in their efforts to classify workers correctly.

According to the DOL, under the economic realities test, most workers are employees subject to the FLSA. You are strongly encouraged to review worker classifications at your organization. The DOL's focus on worker classification, in conjunction with its recent proposed rule regarding the FLSA white collar exemptions, means employers should be prepared for aggressive DOL enforcement of these issues.

## DID YOU KNOW?

Employers looking to eliminate or reduce exposure to employer shared responsibility penalties under the ACA by decreasing employee hours should keep an eye on [Marin v. Dave & Buster's Inc.](#)

Dave & Buster's reduced the work hours of employees to fewer than 30 hours per week, making the plaintiffs ineligible for health coverage. The class action lawsuit claims that Dave & Buster's violated Section 510 of ERISA, which makes it unlawful to discriminate against or interfere with a participant's or beneficiary's rights under the provisions of an employee benefit plan.

The plaintiffs claim that the reduced work hours interfered with their rights under the plan to be eligible for employer coverage.

## Educate Employees on Cyber Security

Employees' lack of cyber security knowledge may pose one of the greatest risks to an organization's network security. Hackers often send "phishing" emails that contain viruses which can then be opened by unsuspecting employees. Also, employees logging on to the company network using an unprotected Wi-Fi connection may open the network to vulnerability.

Properly trained employees are the first line of defense against a cyber attack. HR, working with IT, should consider implementing training for employees on preventing data breaches.

The training for employees should include education on different types of exposures and on how employees can protect against security breaches. Employee training should also include instructions on what to do in the event of a suspected or confirmed cyber attack.

Employee training on cyber security should be a priority for all organizations, regardless of size. Hackers don't discriminate in their targets, and may even go after small and mid-size companies knowing that these organizations frequently have fewer safeguards in place.