HRHero.com
A division of BLR®

FLORIDA
EMPLOYMENT LAW LETTER

Part of your Florida Employment Law Service

Tom Harper, Managing Editor • Law Offices of Tom Harper
Lisa Berg, Andrew Rodman, Co-Editors • Stearns Weaver Miller, P.A.
Robert J. Sniffen, Jeff Slanker, Co-Editors • Sniffen & Spellman, P.A.

Vol. 29, No. 4
June 2017

What's Inside

What's Online

Podcast
"Employee value equation" for performance management
ow.ly/ZqoO30c06if

Strategic HR
Employee network groups can help you improve retention
ow.ly/QsaG30bPGmp

Discipline
Be careful before you discipline for Internet use
http://bit.ly/2r2ieUm

Find Attorneys
To find the ECN attorneys for all 50 states, visit
www.employerscounsel.net

ECN EMPLOYERS COUNSEL NETWORK
EMPLOYERSCOUNSEL.NET

DATA BREACHES

Cyberwarfare in the workplace: HR on the front lines

by Lisa Berg
Stearns Weaver Miller Weissler Alhadeff & Sitterson, P.A.

If you thought cybersecurity was only IT's responsibility, think again. Some of the biggest security threats are from hackers who purposefully target a company's employees and trick them into divulging information or granting access to confidential information. Other threats result from employees' careless mistakes, such as logging on to an unsecured public Wi-Fi hotspot.

When you think about your company's cybersecurity strategy, it is important to remember the human element. More than 50% of all security incidents—i.e., events that compromise the confidentiality, integrity, or availability of an information asset—are caused by people inside the organization. Therefore, HR professionals can play a critical role in thwarting and responding to cybersecurity threats.

Protect your data

Here are helpful measures you can implement to protect your company:

(1) Conduct proper background screening of employees.

(2) Add cybersecurity training to your onboarding process. Educate each new hire about the company's policies regarding the protection of confidential information and the consequences of failing to comply.

(3) Require employees with access to confidential information to sign restrictive covenants (i.e., nondisclosure, nonsolicitation, and noncompetition agreements). Restrict access to confidential information to employees on an "as-needed" basis, and keep records of which employees have access to the data.

(4) Create an inventory of data, and determine proper protections, access, and controls. Data reside not only on servers and at workstations but also on mobile devices, thumb drives, backup systems, and clouds. If you don't know where your information resides, you can't protect it.

(5) Delete data your organization no longer needs to maintain in accordance with applicable data retention laws and regulations.

(6) Work with IT to install encryption and wiping software on all mobile devices, removable media, and electronic devices containing company information that will be used by employees. This step cannot be overlooked since it is likely that an employee will lose a laptop, leave his iPhone on a table, or have his tablet stolen.

(7) Consider instituting a formal system of monitoring the daily activities of employees who have access to data that can be monetized (e.g.,

financial accounts, health information, and Social Security, driver's license, credit card, and bank account numbers).

(8) Hold third parties, vendors, and contractors to the same strict data privacy controls you implement in your organization. Contractors are often targeted by cybercriminals, and their data can be used to infiltrate the target's system. Ensure vendor agreements include language that requires vendors to report potential incidents, cooperate in investigating and resolving security incidents, preserve relevant evidence, allow periodic audits, and maintain relevant insurance.

(9) Adopt security policies that address the Health Insurance Portability and Accountability Act (HIPAA) and comply with national standards. Ensure that your employee handbook has policies that address the following issues:

- The duty of confidentiality;
- Acceptable social media use;
- The duty to report theft or loss of data;
- Ethical conduct;
- An employee bringing his own device;
- Remote access;
- Privacy;
- Wearable technology;
- E-mail, Internet, and computer use;
- Document retention;
- The return of corporate property;
- The obligation to protect third-party (e.g., customer) information; and
- Security measures (e.g., encryption, access limits, and physical locks).

(10) Require complex passwords—meaning at least eight characters with uppercase and lowercase letters, numbers, and special characters. According to a 2016 study by Experian, 63% of confirmed data breaches involve weak, default, or stolen passwords. Work with IT to ensure that employees change their passwords at least four times per year and are not able to use previous passwords.

(11) Establish a mandatory cybersecurity training program to educate your employees on current cybersecurity attack methods, proper handling and protection of company and third-party data, and the consequences of violating company security policies. For example, train employees on how to recognize "phishing" and other forms of social engineering. Social engineering is designed to trick someone into doing something they would not otherwise do. The most successful phishing attempts involve a form of social engineering in which a message (typically an e-mail) with a malicious attachment or link is sent to a victim with the intent of tricking the recipient into opening an attachment or divulging his password. Generally, the user clicks, malware loads, a foothold is gained, and the phisher dictates what happens next. Phishing shows the importance of mandatory, frequent, and repeated training.

(12) Reward employees for spotting intrusion attempts and immediately notifying IT. Encourage self-reporting of breaches.

(13) Create a cybersecurity incident response plan that includes an incident response team. The team should be composed of individuals from key departments, including IT, legal and compliance, HR, risk management, communications/public relations, security, operations, finance, relevant executives, outside legal counsel, and cybersecurity vendors.

(14) Review state and industry regulations on data security and the protection of customers' financial, medical, and personal data.

(15) Use offboarding procedures to minimize the risk of data leakage (e.g., immediately cut off access to your system and change passwords before an employee is notified of his dismissal). Utilize exit interviews with departing employees to retrieve company data from electronic devices, remind them of their contractual obligations, and deter wrongdoing.

(16) Consider investing in cyber liability insurance. Evaluate first-party insurance to cover the company's direct losses from a data breach and third-party insurance to cover certain damages suffered by customers.

(17) Treat employees with dignity and respect. Studies show that nearly 60% of fired employees steal important corporate data on their way out the door. A disgruntled employee can be the most serious vulnerability in your data protection program.

(18) Hold everyone in the organization accountable for cybersecurity compliance. After all, it takes only one untrained person to cause a breach!

Bottom line

An effective cybersecurity program requires participation and buy-in from various departments in an organization, and HR is a critical component of that effort. It's no longer a matter of fearing "if" your organization will experience a data breach, but "when."

Lisa Berg is an employment lawyer and shareholder in the Miami office of Stearns Weaver Miller, P.A. You may reach her at lberg@stearnsweaver.com or 305-789-3543. ✤

ANDY'S IN-BOX

21st century hiring: The times they are a-changin'

by Andy Rodman
Stearns Weaver Miller Weissler
Alhadeff & Sitterson, P.A.

It seems as though I come across an article or blog post concerning technological advances in hiring and recruiting every day. Most of the articles and posts focus on the use of analytics and artificial intelligence in seeking out, recruiting, and hiring qualified applicants.

I recently read an article about a California-based company that outsources a robot, of sorts, to conduct preliminary job interviews. The robot "chats" with applicants by computer or smart phone (similar to a text message conversation) and asks about starting dates, starting rate of pay, and level of experience. If the robot deems an applicant a good fit, it will schedule an in-person interview with a human. Remarkably, the chat is so realistic that even when applicants are told they are communicating with a robot, 72 percent of them still believe they are talking with a human.

Several companies offer to help HR practitioners locate qualified applicants (who may not even be looking for a new job), analyze stacks of résumés to predict which applicants would be the best "fit" in terms of corporate culture and personality, and predict how long each applicant would remain with the company if hired. Many of the vendors use advanced analytics and "big data" to reach their conclusions. It's similar to online marketers' use of advanced analytics to predict your purchasing preferences (which is how retail advertisements magically appear on Facebook and Google).

Is all of this really necessary? Do we really need robots and analytical assistance in the hiring and recruiting process? You may be skeptical, but if you're like me, you also questioned the *need* for the Internet and e-mail (and certainly the need for the Internet and e-mail on a cell phone) in the early to mid-1990s.

So what's wrong with the "old-fashioned" way—having an actual human circulate a classified ad (maybe even online), review applications and résumés, and conduct in-person interviews? Proponents of the use of high-tech products in the hiring and recruiting process point to the following facts:

- Humans may make hiring decisions on factors other than skills and experience, such as gut feeling, intuition, common friends and interests, and even physical attraction.
- Studies show that in workforces lacking diversity, human selection of new hires tends to perpetuate the lack of diversity (perhaps because hiring managers tend to hire people who are "like them").
- The use of high-tech products decreases the amount of time and money spent reviewing résumés and interviewing applicants and increases new-hire longevity.

From a legal standpoint, the law has not caught up to the available technology, and it may take a few years before we see court decisions on a whole host of legal issues. Vendors' status as consumer reporting agencies (and their conclusions as consumer reports) under the Fair Credit Reporting Act (FCRA) and potential disparate impact claims arising from the use of analytics and big data in hiring and recruiting are just a couple of legal issues.

In light of the uncertainty in this area, be sure to consult with your employment counsel before engaging a vendor that uses analytics or big data to assist with hiring or recruiting needs.

Andy Rodman is a shareholder and director at the Miami office of Stearns Weaver Miller. If you have a question or issue that you would like him to address, e-mail arodman@stearnsweaver.com or call 305-789-3255. Your identity will not be disclosed in any response. This column isn't intended to provide legal advice. Answers to personnel-related inquiries are highly fact-dependent and often vary state by state, so you should consult with employment law counsel before making personnel decisions. ✤

WORKPLACE CULTURE

Understand the whistleblower (and prevent retaliation claims)

With retaliation claims again topping the list of charges filed most frequently with the Equal Employment Opportunity Commission (EEOC) and whistleblower claims on the rise, employers can learn a great deal by better understanding the psychology of a whistleblower.

Retaliation is all about perception

In its 2015 enforcement and litigation data, the EEOC revealed that most of the charges filed with the agency nationwide are for retaliation. Continuing a trend from previous years, retaliation claims amounted to almost half of the charges filed with the EEOC—44.5 percent—in fiscal year (FY) 2015.

Whistleblower cases also continue to rise. The Occupational Safety and Health Administration (OSHA) has whistleblower authority to protect workers from retaliation under 22 federal laws, including for reports of bank and securities fraud under the Sarbanes-Oxley Act (SOX) and perceived violations of consumer protection laws under the Consumer Financial Protection Act (CFPA) and the Consumer Product Safety Improvement Act (CPSIA). In FY 2015, OSHA received almost 3,300 whistleblower complaints—an increase of almost 1,000 cases from just five years earlier.

The fact that retaliation charges are more prevalent than any other type of discrimination charge illuminates an interesting phenomenon: The lion's share of claims under the discrimination statutes are not due to discrimination itself but to the perception of adverse treatment of employees who report law and policy violations, including discrimination. That raises a critical question in today's employment law context: How should companies treat whistleblowers?

A rock solid answer is, "Don't retaliate." In addition, be very clear about any actions that could be *perceived* as retaliatory. But the issue is more nuanced with respect to how whistleblowers should be assessed and addressed in litigation. One thing is clear: You must resist the oversimplified view of the whistleblower as a divisive malcontent seeking excuses for a poor employment record. While most whistleblowers are not the noble self-sacrificing heroes they may perceive themselves to be, you should keep in mind that regulatory agencies and juries aren't very likely to question a whistleblower's motives.

The psychology of whistleblowing

A recent research article titled "The Psychology of Whistleblowing" provides some insight into the nuances of dealing with whistleblowers. James Dungan, Adam Waytz, and Liane Young, a group of psychology and management researchers from Boston College and Northwestern University, write, "From one perspective, whistleblowing is the ultimate act of justice, serving to right a wrong. From another perspective, whistleblowing is the ultimate breach, a grave betrayal."

Relying on moral foundations theory, the researchers conducted five studies showing that whistleblowing represents a trade-off between two fundamental moral values: fairness and loyalty. Individuals and situations emphasizing fairness cause whistleblowing to be more common and more supported, and individuals and situations emphasizing loyalty cause whistleblowing to be less common and less supported. So the critical determinant in whether the whistleblower emerges as a hero or a snitch depends on whether the narrative frame prioritizes loyalty or fairness.

One of the studies conducted by the researchers began by using different essays to induce individuals to endorse values of fairness or values of loyalty. Then, the participants were presented with the opportunity to report a coworker in an online marketplace who shirked his work duties. Participants who were primed to embrace fairness blew the whistle on the coworker more often than those who were primed to embrace loyalty. The trade-off between values of fairness and loyalty appeared to drive the decision about whether or not to be a whistleblower.

Personal factors that contribute to whistleblowing

Relying on numerous other studies, the researchers report that certain personality traits and demographic factors contribute to more incidents of blowing the whistle. Factors that correlate with higher rates of whistleblowing include:

- Having a longer tenure of employment at the company;
- Receiving higher pay;
- Being highly educated;
- Being male;
- Being an extrovert; and
- Having a proactive personality.

The researchers conclude that people with more occupational power and whose personality traits support nonconformity are more likely to dissent or blow the whistle. They suggest that the reason for this may be that such individuals face a lower threat of punishment for violating group cohesion.

Situational, cultural factors that may predict whistleblowing

The researchers opine that in addition to personal traits that may affect whether an employee becomes a whistleblower, situational and cultural factors play a

role. For example, predictors of whether a worker will decide to blow the whistle may be determined by the level of organizational support and encouragement for whistleblowing and whether the mechanisms and protections for reporting wrongdoing are well-known by employees.

In addition, differences in cultural norms may affect the likelihood of whistleblowing. For instance, people from many Asian cultures view whistleblowing less favorably than individuals from the United States.

Cultivate a culture of criticism that leads to loyalty

Employers already understand the need for policies that don't merely prohibit discrimination but also prohibit retaliation and the adverse treatment of whistleblowers. But it isn't enough to just *allow* whistleblowing or even to *inform* workers that they are protected from retaliation. Instead, the researchers encourage companies to create a culture that supports internal criticism across the spectrum of issues, large and small. They share research showing that whistleblowing can either increase cooperation and reduce selfishness within the group or increase dissent and denigration, reducing group harmony. The difference comes down to group culture.

Organizations looking to reduce the threat of retaliation lawsuits should consider creating a culture that welcomes criticism. The thought is that if you encourage employees to blow the whistle internally and dissent is viewed as a good thing that's valued by your company (i.e., it makes the company better), loyalty is enhanced, and whistleblowing to an outside entity such as the EEOC or OSHA becomes less likely.

Part of that effort should include strong, well-publicized policies that encourage internal reporting of potential violations or wrongdoing. But it should also include training supervisors on how best to welcome criticism and avoid retaliation toward subordinates who speak up, in addition to conveying other messages that highlight the value of internal constructive criticism.

Make whistleblowing 'less noble, more normal'

If an employee's whistleblower or retaliation claim heads to court, you might benefit from evaluating your complex feelings toward the whistleblower. You may not want to explicitly play the loyalty card because blaming the employee for breaking ranks may seem to reinforce his argument that your company had a retaliatory motive. Instead, seek to normalize the act of whistleblowing.

If your company has embraced a culture of criticism, you should be able to point to several features of your policies and culture that don't just allow whistleblowing but positively encourage it. The ability to prove that such a culture exists permits you to suggest that whistleblowing isn't a uniquely noble act on the employee's part but is instead something you expect of all your employees. The fact that a claim was made means that you

AGENCY ACTION

USCIS announces efforts against H-1B abuse. U.S. Citizenship and Immigration Services (USCIS) in April 2017 announced stepped-up measures to fight H-1B visa fraud and abuse. Also, on April 7, the agency announced it had reached the congressionally mandated 65,000 H-1B visa cap for fiscal year 2018. It also announced it had received a sufficient number of H-1B petitions to meet the 20,000-visa U.S. advanced degree exemption, also known as the master's cap. The antifraud measures will target cases in which USCIS can't validate the employer's basic business information through commercially available data, H-1B-dependent employers, and employers petitioning for H-1B workers who work off-site at another organization's location. The agency said targeted site visits will allow it to focus resources where fraud and abuse of the H-1B program may be more likely to occur.

EEOC examines state of current, future workforce. The Equal Employment Opportunity Commission (EEOC) heard from workforce experts about challenges posed by a skills gap and lack of opportunities during a public meeting in April. "A thorough understanding of today's workforce, the employment opportunities available, the challenges in the job market—all are critical to our work in the EEOC," Acting Chair Victoria A. Lipnic said after the meeting. "Job opportunities must not be denied to anyone for discriminatory reasons. And at the end of our work, discrimination must be remedied with employment opportunity." Speakers at the meeting discussed the changing nature of work creating a gap between jobseekers and vacancies, the impact of technology, and the need to remove barriers for people with disabilities.

OSHA delays enforcing crystalline silica standard. The Occupational Safety and Health Administration (OSHA) announced in April that it would delay enforcement of the crystalline silica standard that applies to the construction industry. The delay will allow time to conduct additional outreach and provide educational materials and guidance for employers. The agency said it wants additional guidance because of unique requirements in the construction standard. Originally scheduled to begin June 23, enforcement is now set to begin September 23. OSHA said it expects employers in the construction industry to continue to take steps either to come into compliance with the new permissible exposure limit or to implement specific dust controls for certain operations as provided in Table 1 of the standard. Construction employers also should continue to prepare to implement the standard's other requirements, including exposure assessment, medical surveillance, and employee training. ✤

need to take it seriously, but it doesn't mean that you retaliated against the employee.

Ultimately, the complexity of our views of whistleblowers is a reminder that employment decisions and court cases are not just about claims, evidence, and the law. They're also about perceptions and a story and how each of the parties fits within that story's moral frame. ✤

WAGE AND HOUR LAW

How much 'side work' can employees do and still be paid tipped minimum wage in FL?

by Tom Harper
The Law and Mediation Offices of
G. Thomas Harper, LLC

In a May 18, 2017, decision, Federal District Judge James Moody upheld the U.S. Department of Labor's (DOL) rule that a tipped employee may be paid a direct wage that is less than the Florida minimum wage of $8.10 per hour only if he spends no more than 20% of his time on duties that do not directly result in tips.

Background

Under the Fair Labor Standards Act (FLSA), the federal wage and hour law, employers may claim a "tip credit" toward satisfying their minimum wage requirements for tipped employees. That means tips are credited against—and satisfy a portion of—employers' obligation to pay minimum wage. However, Florida's minimum wage currently is $8.10 per hour, higher than the federal minimum wage of $7.25 per hour.

The Florida Constitution provides: "For tipped Employees meeting eligibility requirements for the tip credit under the FLSA, employers may credit towards satisfaction of the Minimum Wage tips up to the amount of the allowable FLSA tip credit in 2003." In 2003, the FLSA's tip credit was $3.02. At the time, the federal tip credit was calculated by subtracting the federal reduced minimum wage of $2.13 from the federal minimum wage of $5.15. Therefore, under the Florida Constitution, the tip credit can be no more than $3.02.

Although the Florida minimum wage has increased, the $3.02 tip credit has stayed the same. Thus, the direct wage (also called the subminimum wage) that must be paid to employees has also increased. As of January 1, 2017, the direct wage was $5.08—the Florida minimum wage ($8.10) minus the 2003 tip credit ($3.02). Thus, employers are required to pay only $5.08 per hour to tipped employees who meet certain requirements. The rest of the minimum wage is made up by tips employees collect.

Job in question

Robert Eldridge worked as a server and bartender at Outback Steakhouse in St. Petersburg. He sued his employer, OS Restaurant Services, LLC, a/k/a Outback Steakhouse of Florida, LLC, for unpaid wages and overtime. He claimed that he spent more than 20% of his time on manual duties that were not directly related to receiving tips and that his employer violated the law by paying him the reduced minimum wage and using the tip credit to make up the difference. He argued that since he spent more than 20% of his time on side duties, he should have been paid the full minimum wage, not the tip credit wage. The employer moved to dismiss the suit, claiming the DOL's 20% rule did not apply. The court ruled that the 20% rule applied and refused to dismiss Eldridge's claims.

Eldridge claimed his employer violated Florida law by paying him the subminimum wage for duties that did not result in tips. The court agreed. Eldridge claimed that performing the following duties took more than 20% of his work time:

- Bar set-up assignments (e.g., brewing coffee and washing dirty glassware);
- Table set up and break down and cleaning projects (e.g., cleaning and wiping down table tops);
- Maintenance and janitorial undertakings (e.g., placing trash cans in designated areas); and
- Undesignated skeleton crew duties to maintain restaurant performance and reduce overhead and labor costs.

In deciding whether Eldridge's claim was valid, the court looked to the DOL's regulations, which took effect in April 2011. The regulations provide that if an employee is engaged in two occupations (one tipped and one nontipped), the employer may not take the tip credit for hours worked in the nontipped occupation. On the other hand, the regulations go on to state that "a waitress who spends part of her time cleaning and setting tables, toasting bread, making coffee and occasionally washing dishes or glasses" is still subject to a tip credit.

The 20% rule came from the 1988 DOL Field Operations Handbook, which states that employees who spend more than 20% of their time performing general preparation work or maintenance are not subject to a tip credit for the time spent performing those duties. Outback Steakhouse argued that the 20% rule was not binding authority in Florida. Indeed, the court acknowledged that the federal court of appeals with jurisdiction over Florida has never ruled on the issue.

The court found that a number of federal courts have sided with the DOL and ruled that its interpretation is reasonable. The U.S. 8th Circuit Court of Appeals stated, "The regulation places a temporal limit on the amount of related nontipped work an employee can do

and still be considered to be performing a tipped occupation." The 8th Circuit found that the 20% rule was a reasonable way to interpret terms like "part of the time" and "occasionally." Thus, the Florida court upheld the 20% rule and denied Outback Steakhouse's motion to dismiss. *Eldridge v. OS Restaurant Services, LLC a/k/a Outback Steakhouse of Florida LLC,* No: 8:17-CV-798-T-30TGW (M.D. Fla., May 18, 2017).

Remember these points

The DOL regulations state that an employer must provide the following information to tipped employees before using the tip credit:

(1) The cash wages the employer will pay tipped employees (in Florida, at least $5.08 per hour);

(2) The amount claimed by the employer as a tip credit (in Florida, at least $3.02 per hour);

(3) An explanation that the tip credit claimed by the employer cannot exceed the amount of tips received by tipped employees;

(4) An explanation that all tips received by tipped employees are to be retained by employees (except for valid tip-pooling arrangements that are limited to employees who customarily and regularly receive tips); and

(5) A statement that the tip credit will not be applied to tipped employees unless they have been informed of the tip credit provisions.

Under the DOL regulations, the employer may inform tipped employees of the tip credit provisions by oral or written notice. Further, the regulations state an employer must be able to show it has provided notice. The regulations also state that if an employer fails to provide the required information, it cannot use the tip credit and must pay tipped employees at least $7.25 per hour ($8.10 per hour in Florida) and allow them to keep all tips received. Provide written notice to make it easy to prove that you gave notice to employees.

Employers electing to use the tip credit must show that tipped employees were paid at least minimum wage when direct (cash) wages and the tip credit are combined. If an employee's tips and direct wages do not equal $8.10, the employer must make up the difference.

Tip pooling

The DOL regulations allow for tip pooling among employees who customarily and regularly receive tips, such as servers, bellhops, and bartenders. Conversely, a valid tip pool may not include employees who do not customarily and regularly receive tips, such as dishwashers, cooks, chefs, and janitors. Employee interaction with customers is one factor that helps determine who may be included in a tip pool. The regulations state that if a tipped employee is required to contribute to a tip pool that includes workers who do not customarily and regularly receive tips, the employee is owed all tips she contributed to the pool and the full $8.10 minimum wage.

One positive aspect: The regulations do not impose a maximum contribution amount or percentage on valid mandatory tip pools. However, the employer must notify tipped employees of a required tip-pool contribution amount and may take a tip credit only for the actual tips each tipped employee ultimately receives.

Whose tip is it?

The regulations state that tips are the sole property of tipped employees regardless of whether the employer takes a tip credit. The regulations prohibit any arrangement between the employer and tipped employees in which tips become the property of the employer. The DOL's 2011 final rule amending its tip credit regulations specifically sets out the Wage and Hour Division's (WHD) interpretation of the FLSA's limitations on an employer's use of employees' tips when a tip credit is not taken. The rule states in pertinent part:

> Tips are the property of the employee whether or not the employer has taken a tip credit. The employer is prohibited from using an employee's tips, whether or not it has taken a tip credit, for any reason other than that which is statutorily permitted: as a credit against its minimum wage obligations to the employee, or in furtherance of a valid tip pool.

Service charges

A compulsory charge for service (e.g., a charge placed on a ticket when the number of guests at a table exceeds a specified number) is not a tip. Service charges cannot be counted as tips, but they may be used to satisfy the employer's minimum wage and overtime obligations under the FLSA. If an employee receives tips when a compulsory service charge is added, the tips may be considered in determining whether he is a tipped employee and in applying the tip credit.

TRAINING CALENDAR

Call customer service at 800-274-6774 or visit us at the websites listed below.

SAFETY CULTURE 2017:
Buy-In, Behavior, and Other Keys to Making Safety Stick
http://store.HRhero.com/safety-culture-conference
Austin, Texas, September 11-12

CAL/OSHA SUMMIT 2017:
Leading-Edge Strategies for Exceptional Safety Management and Compliance in California
http://store.HRhero.com/cal-osha-summit
Costa Mesa, October 10-11

12TH ANNUAL CALIFORNIA EMPLOYMENT LAW UPDATE
http://store.HRhero.com/california-employment-law-update
Costa Mesa, October 11-13

ADVANCED EMPLOYMENT ISSUES SYMPOSIUM 2017
http://store.HRhero.com/aeis
Las Vegas, November 15-17

WORKFORCE LEARNING & DEVELOPMENT 2017:
Train. Retain. Excel.
Las Vegas, November 16-17
http://store.HRhero.com/workforce-learning-conference

WEBINARS & AUDIO SEMINARS
Visit http://store.HRHero.com/events/audio-conferences-webinars for upcoming seminars and registration.

7-11 Achieving Competitive, Fair Pay: Compensation Strategy Tips for Filling Open Positions While Meeting Market Demands

7-13 Severance Agreements: When to Use Them and How to Draft Them to Limit Company Liability

7-14 Traveling Employees: Your Duty of Care and the Major Mistakes to Avoid While Workers Are Traveling or Working Abroad

7-19 Today's Topsy-turvy Labor & Employment Landscape: What's Changing & Staying the Same Under New the DOL Secretary & EEOC/NLRB Chairs ✤

If tips are placed on a credit card and the employer pays the credit card company a fee, the employer may deduct the fee from the employee's tips. Further, if an employee does not receive sufficient tips to make up the difference between the direct wages and the minimum wage, the employer must make up the difference. If an employee receives only tips and is not paid a cash wage, the employer owes the full minimum wage.

Deductions

Deductions from an employee's pay for walkouts, breakage, or cash register shortages that reduce her wages below the minimum wage are illegal. If a tipped employee is paid $5.08 per hour in direct wages and the employer claims the maximum tip credit of $3.02 per hour, no deductions can be made without reducing the employee's pay below the minimum wage (even if she receives more than $3.02 per hour in tips).

Computing overtime for tipped employees

If the employer takes a tip credit, it must calculate overtime based on the full minimum wage, not the lower direct wage. The employer may not take a larger tip credit for overtime hours than for straight-time hours. For example, if an employee works 45 hours during a workweek, he is owed 40 hours at $5.08 in straight-time pay and five hours of overtime at $9.13 per hour ($8.10 x 1.5 - $3.02 in tip credits).

Bottom line

The rules for paying tipped employees are so complicated and fraught with potential pitfalls that some employees' attorneys specialize their practices in challenging these pay systems. While common mistakes may not amount to much money per employee, liability can add up to big dollars when mistakes involve many employees over several years. Take care to audit your pay systems periodically, train your employees on proper pay procedures, and respond to any employee complaints or concerns about pay—before they turn into a lawsuit.

You may contact the author at tom@employmentlawflorida.com. ✤

FLORIDA EMPLOYMENT LAW LETTER (ISSN 1041-3537) is published monthly for $447 per year plus sales tax by **BLR®—Business & Legal Resources,** 100 Winners Circle, Suite 300, P.O. Box 5094, Brentwood, TN 37024-5094.

Editorial inquiries should be directed to G. Thomas Harper at The Law and Mediation Offices of G. Thomas Harper, LLC, 1912 Hamilton Street, Suite 205, Post Office Box 2757, Jacksonville, FL 32203-2757, 904-396-3000. Go to www.EmploymentLawFlorida.com for more information.

For questions concerning your subscription or Corporate Multi-User Accounts, contact your customer service representative at 800-274-6774 or custserv@blr.com.

HRhero® a division of BLR BLR®