

page 2
New law reaffirms right to post
negative reviews online
Conduct a website self-audit to
ensure compliance with the ADA

page 3
Take care with COBRA compliance
— or pay big damages

page 4
Tips for avoiding a data breach

Legal Matters®

Business Law
spring 2017

Social media endorsements: How to pay influencers to endorse your brand

It's becoming popular for companies to pay social media users with big followings to endorse their products or share content about their brand. It's a great way to get your message out to a wider network of customers in an authentic way.

But the Federal Trade Commission (FTC) is paying attention and enforcing rules that say you can't do it without disclosing the relationship.

Recently, the FTC reached settlements with such brands as Lord & Taylor and Warner Bros. Home Entertainment over their failure to disclose such relationships.

In the Lord & Taylor case, the company paid influencers up to \$4,000 for an endorsement without disclosing the relationship, in clear violation of the FTC rules.

However, in many situations it's not quite as clear, such as when a business trades merchandise or a promise of future payment for an endorsement on Instagram. It's also complicated when the social media influencers don't have clear sponsorship agreements with the brand.

Still, the FTC asserts that consumers have a right to know whether the so-called influencer is commenting about a product of his or her own volition, or whether he or she was given the product for free in exchange for reviewing it.

In addition, the consumer advocacy group Public Citizen is raising awareness about potentially unfair advertising practices on



©thinkstockphotos.com

social media and has been asking the FTC to pay closer attention to content from influencers, particularly on Instagram.

The group recently requested an FTC enforcement action against both paid influencers that fail to disclose and the brands that hired them in the first place.

Regardless of any action the FTC takes on that request, brands would be wise to disclose their relationships with social media influencers, no matter what the relationship is or what was exchanged.

To avoid an FTC violation, you must disclose any "material con-

continued on page 2

WALTERS LEVINE & LOZANO

Sarasota office: (941) 364-8787 • Tampa office: (813) 254-7474
Jacksonville office (813) 455-8615 • Chicago office: (312) 782-8807
www.walterslevine.com

New law reaffirms right to post negative reviews online

Under a new federal law, individuals have a right to post truthful negative reviews about a product or service provider. That's the case even if they previously signed an agreement that prohibited such reviews.

Over the past few years, this controversial business practice of including non-disparagement clauses in contracts or terms of service has led to a number of lawsuits. These so-called "gag clauses" are intended to deter customers from writing negative reviews and require them to pay a fee if they do so despite the contract.

The new Consumer Review Freedom Act bars companies from using these clauses. It gives the Federal Trade Commission and the states the power to enforce the law, allowing them to take legal action against businesses that fail to remove these clauses from their contracts.

The Better Business Bureau already had prohibited accredited businesses from using gag clauses.

Yelp, TripAdvisor and several other entities that regularly post consumer reviews have stated their support for the new legislation.

Conduct a website self-audit to ensure compliance with the ADA

Over the past couple of years, more than 200 plaintiffs have sued businesses nationwide arguing that their websites fail to provide access to people with certain disabilities, alleging a violation of the Americans with Disabilities Act. More recently, a law firm based in Pittsburgh sent demand letters to businesses, banks and others saying that they were willing to "work constructively" toward compliance for a fee.

While court rulings on whether the ADA applies to websites have been mixed, plaintiffs have been using the rulings in their favor to persuade businesses to settle.

The ADA, which went into effect in 1990, prohibits discrimination against people with disabilities. Title III of the Act prohibits discrimination on the basis of disability in "places of public accommodation." The law doesn't specifically mention websites, but some plaintiffs argue that a website should be treated as a "place of public accommodation."

The Department of Justice, which is tasked with enforcing the ADA, has not issued any rules to date for website compliance. Businesses have been waiting for these guidelines for years, but they are not expected until 2018.

In the interim, it's better to be safe than sorry in protecting your business against these kinds of allegations. That means that all businesses should self-audit their websites to ensure they are accessible to individuals with disabilities.

The rules to follow in conducting your audit are known as the Web Content Accessibility Guidelines (WCAG-2.0) Level AA. These guidelines include recommended alternatives to your usual text, such as increasing font size, using braille or including pre-recorded audio-only or video-only content.

There are also sites that will essentially assess your website for you and provide a report explaining any accessibility concerns.

You might need a web developer to help you implement changes. It's also important to document any changes you make as a further indication of your focus on accessibility.

Businesses should make sure their insurance policies cover website accessibility claims. Some policies include a broad exclusion for discrimination suits.

An attorney can help you ensure your site is compliant with the guidelines and assist you in reviewing your insurance coverage.

How to pay influencers to endorse your brand

©thinkstockphotos.com



continued from page 1

nection" between your brand and an influencer every time an endorsement is made. That includes payment, future payment, a new product preview, free products or anything else.

That can easily be done using a hashtag. The hashtag

must be "clearly and conspicuously" presented, as defined by how consumers would understand the disclosure. For example, #ad or #advertisement or #sponsoredpost would likely meet the standard.

To be even more clear, be sure to put hashtags before a video or post instead of after, so they don't get buried. A note of thanks to the company for the product isn't enough without the hashtag disclosure.

Take care with COBRA compliance — or pay big damages

In recent months, at least four companies have gotten into trouble for failing to provide Consolidated Omnibus Budget Reconciliation Act of 1985 (COBRA) notices to health plan participants.

Suits of this nature can lead to big damages. Since 2015, courts have approved settlements ranging from \$290,000 to \$1 million.

Damages include statutory penalties of \$110 per day, awards to qualified beneficiaries as relief for damages that occur due to the failure to provide an adequate COBRA notice, and attorney fees. The IRS can also assess excise tax penalties of up to \$200 per day for each day that a plan fails to comply with COBRA.

The recent litigation is over two issues: 1) whether qualified beneficiaries have been given the initial COBRA notice and/or the COBRA Election Notice in a timely fashion, and/or 2) whether the notices' content was adequate.

One recent case involves SunTrust Bank, which was sued for failing to send proper COBRA election notices after employees' employment was terminated. The bank's agent, Xerox HR Solutions, sent the notices in a timely manner, but two former employees claimed the notices were "misleading and confusing."

While the notice sent the former employees to a website to elect COBRA coverage, they said they couldn't understand how to make the election. As a result, they didn't obtain coverage.

The two former employees sought class action status for their lawsuit against SunTrust.

The Department of Labor's COBRA notice regulations include 14 content requirements.

The former employees argued that the COBRA notice they received was legally insufficient because it didn't adequately address two of those requirements. They claimed that the notice: 1) failed to provide the COBRA election procedures or election forms; and 2) failed to state the name and address of the party responsible for administration of COBRA benefits.

Both of the former employees said they couldn't find the election form on the website because it was a general human resources website that wasn't specific to COBRA. They sought statutory penalties and attorney fees.

SunTrust settled the lawsuit for \$290,000. In addition, it was required to pay \$103,556 in attorney fees and costs.

The case is a wake-up call for businesses to review their procedures for COBRA notices to avoid expensive mistakes.

When an employee terminates employment, two notices are required, the COBRA General Notice and the COBRA Election Notice.

The COBRA General Notice lays out group health plan participants' general rights and obligations under COBRA. Covered employees and their spouses must be given this notice within their first 90 days of coverage under a group health plan. Employers often include it in their Summary Plan Description.

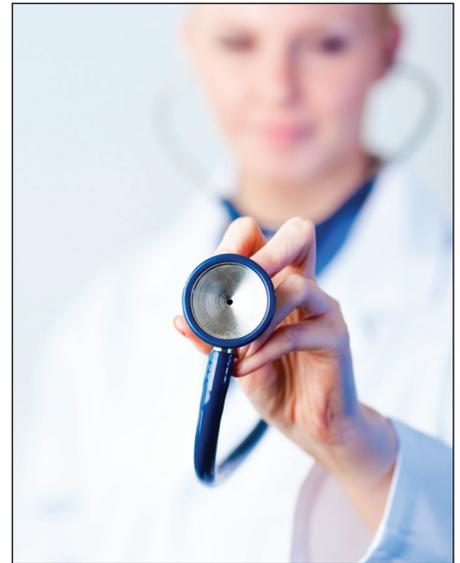
The COBRA Election Notice informs qualified beneficiaries about their rights and obligations with respect to a specific qualifying event, such as termination of employment, an employee's entitlement to Medicare, divorce or legal separation from a covered employee, loss of dependent child status or death of the covered employee.

Employers are required to notify their plan administrator within 30 days of the qualifying event, except in the case of divorce or legal separation from the covered employee and loss of dependent child status. In those instances, the individual must provide the notice.

In turn, the plan administrator must provide an Election Notice to each qualified beneficiary who loses plan coverage in connection with the qualifying event within 14 days after the administrator receives notice.

The Department of Labor has published model COBRA General Notices and Election Notices on its website. Properly completed versions of these notices provide a "safe harbor" for compliance with the COBRA notice content requirements. Other COBRA notices include the Notice of Unavailability of COBRA, used when a request for COBRA coverage is denied, the Notice of Early Termination of COBRA and the Notice of Insignificant Payment of COBRA Premiums.

Enlist the help of an attorney to ensure that your notices are compliant. Pay attention to all of the details to avoid being sued.



©thinkstockphotos.com

We welcome your referrals.

We value all of our clients. While we are a busy firm, we welcome your referrals. We promise to provide first-class service to anyone that you refer to our firm. If you have already referred clients to our firm, thank you!

Tips for avoiding a data security breach

Regardless of the size of your business, it's critical that you work proactively to protect the sensitive and private information of your customers, clients and employees.

While you might hear more often about data breaches at bigger companies, the reality is that smaller companies and organizations are often targeted and typically have limited data security protections in place.

Your approach to protecting your company from a data breach must be comprehensive.

First, be sure to restrict access to sensitive, confidential information only to employees whose job requires that access.

Vendors, many of whom have access to sensitive information, must be screened to ensure they have security

measures in place to protect the data and that they are using your company's data only in relation to providing the specific services for which you have engaged them.

All employees must be trained on your data security policies to give them clarity on what types of information are considered private, what procedures to use to store or dispose of sensitive information, how to report suspicious emails and what the rules are for careful creation and usage of passwords.

If you allow employees to use their personal mobile devices for business purposes, consider restricting how they are used to access your company's data. There is software that can be used to separate personal data from business data on the device. It can also be used to scrub a device if it is misplaced or stolen.

Other protections you should put in place include firewalls to protect your networks, secure WiFi access and encryption of sensitive data.

©thinkstockphotos.com

