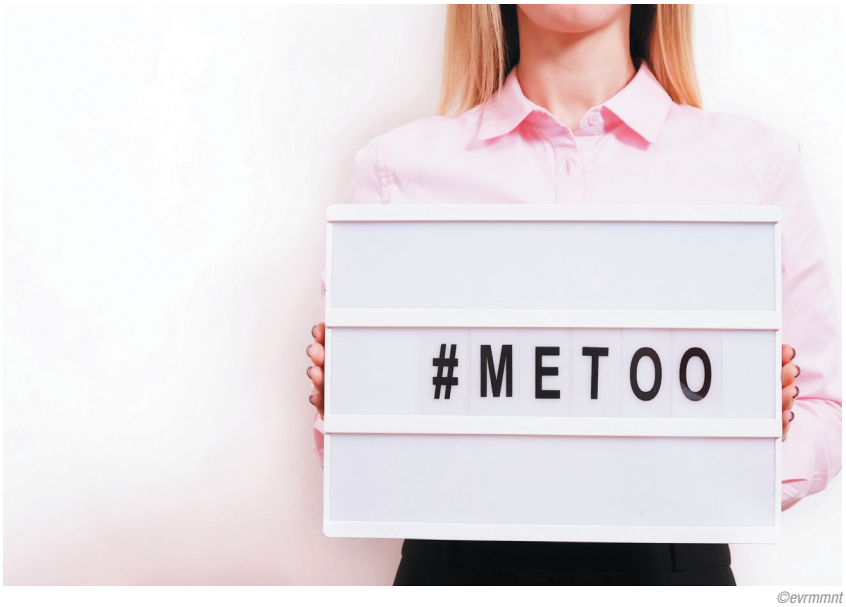
Legal Matters®

Employment
spring 2019

Employers take note: Harassment claims were on the rise last year

Last fall, nearly a year after the #MeToo movement emerged as a major social force, the Equal Employment Opportunity Commission released findings that sexual harassment claims had risen sharply during fiscal year 2018.

The EEOC reported a 12 percent increase in sexual harassment complaints filed with the agency, the first time in a decade when that figure rose. EEOC attorneys filed 41 sexual harassment lawsuits on the agency's behalf, twice as many suits as in 2017. "Reasonable cause" findings — an EEOC determination that there's good reason to believe that harassment occurred — rose by more than 20 percent. Meanwhile, monetary awards recovered by the EEOC for harassment victims increased by more than 20 percent.



©evrmmnt

This shouldn't be surprising. The #MeToo movement and all the publicity surrounding disgraced celebrities, politicians and other public figures has clearly empowered victims to come forward when in the past they might have stayed silent. A decade ago, a study showed that 75 percent of employees who reported mistreatment in the workplace experienced some form of retaliation, which can explain such reluctance. But with the landscape changing, these are dangerous times for any employer that doesn't have a good system in place to prevent sexual harassment from occurring and to address it when it does. This system needs to be both legal (official policies) and cultural (examining

continued on page 3

ALLRED, BACON, HALFHILL & YOUNG, PC

11350 Random Hills Road, Suite 700 | Fairfax, VA 22030
(703) 352-1300 | admin@abhylaw.com | www.abhylaw.com

Case highlights importance of protecting secret documents

©addricky

Does your company have important trade secrets it wants to protect? If so, be sure to take affirmative steps to actually maintain the secrecy of these documents. That can help you if you need to take an ex-employee to court for trade secret violations, as a recent South Carolina case shows.

In that case, employee Diego de Amezega worked for AirFacts, a revenue-accounting software developer for the airline and travel industry, from 2008 to 2015.

His employment agreement required him to return all company property, including documents, upon his departure. But on his last day on the job, he apparently emailed a spreadsheet containing proprietary information about the company's database modeling to his personal email account.

A month later, he allegedly used his AirFacts employee credentials to remotely log into the company's system and download two flowcharts he created while he worked there. Meanwhile — despite having signed an agreement not to work for a competitor for at least a year after leaving the company — he took a job with the American Airlines refunds department less than three months after leaving AirFacts.

AirFacts took de Amezega to federal court, claiming he violated his employment agreement and misappropriated trade secrets. After a five-day trial, a judge ruled that his work with American wasn't similar enough to be considered working for a competitor. The judge also found that the flowcharts he downloaded contained public information and were available to enough AirFacts employees, including de Amezega himself while he worked there, that they were not considered trade secrets.

But a federal appeals court reversed the decision with respect to the trade secrets violation. According to that court, the way de Amezega arranged the data in the flowcharts when he created them gave them an inherent value beyond what the public could see. But more importantly, the court noted that the company took significant steps to maintain the secrecy of the flowcharts, such as requiring all employees to sign confidentiality agreements, putting monitoring software on every computer to track employee access to the flowcharts and giving only certain employees access to the flowcharts in the first place.

If you have proprietary information that you want to make sure is treated as such in court, you absolutely should make an appointment with an employment attorney who has trade-secret expertise.

Beware the careless employee review

Annual or semi-annual employee reviews can be helpful in documenting worker issues to justify actions you might take, and in protecting yourself against potential lawsuits by disgruntled workers. They also can help your workforce identify ways to improve its productivity and professionalism.

But if you go about the review process the wrong way, you may turn what you view as a shield against employment suits into a sword for terminated, transferred or demoted workers. That's because they can use employee reviews as evidence to show you treated them differently from another worker with similar qualifications and that you did so based on their race, religion, ethnicity, gender, disability or other membership in what's known as a protected class.

This is why it's important to have an employment lawyer audit your review process and help you create a review policy to ensure that all reviews back up your assessments with meaningful performance metrics.

For example, you want to make sure a review shows not only how many projects an employee completed, but whether they met or exceeded expectations or whether they fell short and why. It's best to have criteria that are as objective as possible. That way, if an employee is justifiably passed over for a promotion in favor of someone else and claims you discriminated against him based on his membership in a protected class, you have evidence to help counter the allegations. If, however, your documentation is vague and subjective, it provides fuel for the employee.

Additionally, you want to make sure your reviews are consistent. For instance, do employees with similar responsibilities have different supervisors? Make sure your managers are provided specific, objective evaluation criteria and are trained on how to use them, and that you're documenting such training. That way, the reviews provide a meaningful comparison not only for helping you make personnel decisions but to demonstrate to a court that you're treating employees fairly.

Finally, it goes without saying that all reviews should be written, dated, signed and kept on file. Talk to an employment lawyer where you live to find out more.

Employers take note: harassment claims on the rise last year

continued from page 1

your company's work environment and addressing problems).

On the legal front, it would be a good idea to give an employment attorney a call to take a look at your existing policies to ensure each of the following:

• *They're easily understood*

A common mistake companies make is to write important policies in lawyerly language. Such policies might comply with the law, but they can be confusing to employees. Instead, you want your policies written in a way your employees and managers can understand. For example, you need to clearly explain what sexual harassment is and then give examples (i.e. dirty jokes, inappropriate touching and sharing content of a sexual nature). You also need to make clear that these rules apply among co-workers both at work and outside, and that they apply to any form of communication, in-person, electronic or otherwise.

• *You have a clear reporting structure*

Make it clear that any incident should be reported immediately, whether by the victim, a witness or someone the victim told. Provide a clear list of names and contact information for everybody in the reporting structure.

A common mistake companies make is to write important policies in lawyerly language. Such policies might comply with the law, but they can be confusing to employees.

• *Consequences are clear*

Don't be vague. Let it be known that harassment will not be tolerated in the workplace and that any incident can lead to discipline, including termination.

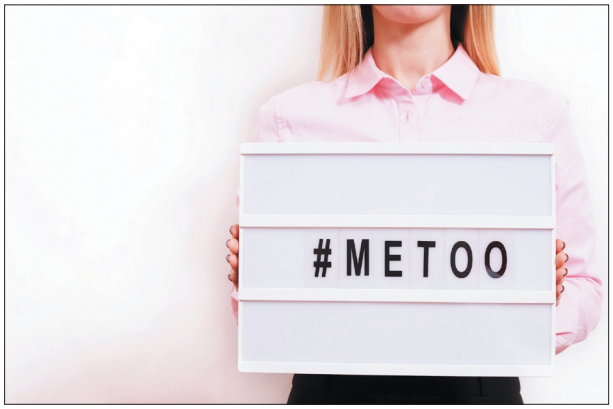
• *You've warned against retaliation*

Make clear to managers that any retaliation for reporting harassment is prohibited and will be punished. Make clear to employees that their complaint will be thoroughly and sensitively investigated and that they won't suffer retaliation for reporting an incident.

On the cultural front, it's equally important to talk to an attorney about how to ensure your workplace can effectively enforce its policies. A few things to discuss include:

• *Training new workers*

It's critical not only to distribute your policy to all new employees, but also to train them on harassment, proper workplace behavior and helping prevent harassment before it starts. Don't assume their prior place of employment had adequate policies or provided such training.



©evrmmnt

• *Reinforcement for existing workers*

Make sure you're redistributing your policy to each employee annually, posting notices of your policy in places where it'll be seen (for example, in the breakroom or lunchroom) and providing annual retraining.

• *Special training for managers*

One of the most common issues leading to harassment liability is poor decision-making by managers. They'll need the same training as other workers, but they'll also need additional training on the unique responsibilities they have.

• *Encouraging 'bystander' intervention*

Beyond teaching workers to recognize harassment and report it when it occurs, train them to intervene and correct coworkers who are stepping too close to the line. This may head off bad behavior before it gets out of hand, and it can improve workplace culture and morale, making for a more professional and productive environment.

While none of this precludes all incidents of harassment, it makes it far less likely that your company will face legal liability in a harassment case or become embroiled in litigation at all After all, even if you win in court, litigation can cost you a lot in terms of time, money and bad publicity. Talk to an employment lawyer where you live to learn more.

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!

ALLRED, BACON,
HALFHILL & YOUNG, PC
11350 Random Hills Road, Suite 700 | Fairfax, VA 22030
(703) 352-1300 | admin@abhylaw.com | www.abhylaw.com


©welcomia

Workers can sue employer for failing to protect personal data

In a ruling that should make employers everywhere sit up and take notice, the Pennsylvania Supreme Court recently decided that workers could bring a negligence claim (in other words, a lawsuit alleging that they were hurt by their employer's unreasonable carelessness) against their employer over a data breach that compromised their personal information.

The case involved more than 60,000 current and former employees of the University of Pittsburgh Medical Center (UPMC). Hackers broke into the UPMC's computer systems and stole employees' names, birthdates, Social Security numbers, salary records, bank information and tax information. The hackers then used this information to file false tax returns in employees' names in order to receive tax refunds.

The employees brought a lawsuit against UPMC in state court seeking to be compensated for damages stemming from the fraudulent returns and the increased exposure to identity theft that the breach caused them. According to the employees, proper firewalls, data encryption and stronger authentication protocols could have prevented the harm. They also argued that they were required to provide information to the employer as a condition of employment, giving the employer a duty to safeguard the information.

UPMC moved to have the case thrown out, arguing that state law doesn't recognize negligence claims by employees in situations that don't involve any physical injury or property damage. Because this case only involved economic losses, it had to be dismissed, UPMC argued.

The trial judge agreed and dismissed the lawsuit, and a midlevel appeals court affirmed the decision.

But the Pennsylvania Supreme Court reversed the ruling and ordered that the suit be reinstated. According to the high court, the duty to act with reasonable care toward those who could foreseeably be hurt by your failure to do so applied to this situation.

This is one decision by a court in one state. However, this reasoning could potentially apply elsewhere too. Call an employment lawyer in your state to discuss your own data-security issues and what kinds of legal exposure they could potentially create for you.