Legal Counsel *for* Churches
Corporate Governance for Churches and Their Leaders

Churches Can Be Liable for Third Party Harassment

In a recent North Carolina case, a Federal Court determined that an employer can be liable for the harassment of its employees by third parties. This case illustrates the importance of churches as employers to monitor the conduct of others who have contact with their employees.

In this case, an employer was found negligent for allowing a customer to harass an employee. The court found that the employer knew of the harassment. The employee complained to the customer and the employer. Yet the employer failed to intervene to stop the harassment. As a result, the employee suffered emotional and physical distress.

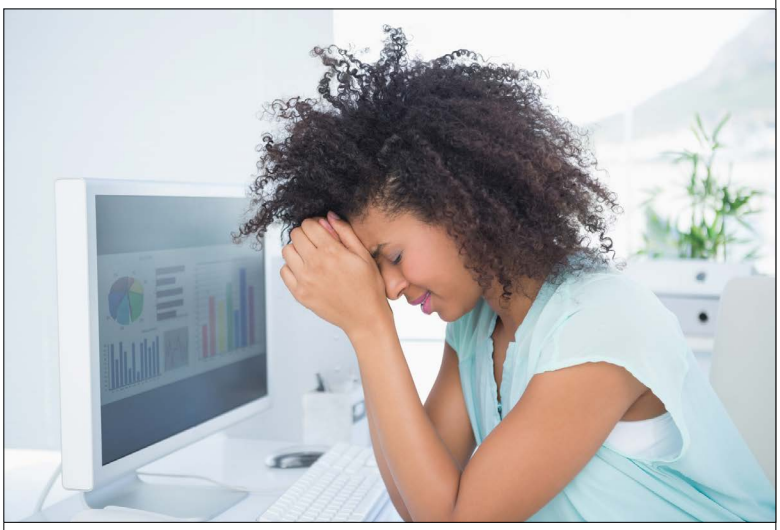
If your church has employees, you have a duty to ensure a safe work environment. Employees should be trained and regularly reminded to treat each other with respect. This is the law. In this instance, courts may now make your church accountable for the treatment your employees receive from others.

Third-party harassment of employees can come from several sources. Vendors who provide services to your church often have access to your staff. Church employees also interact with church members and others in the community. Ensuring church staff is protected from harassing treatment is an employer's obligation.

Under Title VII of the Civil Rights Act of 1964, an employer is liable for third parties who create a hostile work environment if the employer knew or should have known of the harassment and failed to take prompt remedial action reasonably calculated to end the harassment.

> "The Church is subject to liability for what it knows or should have known."

In general, a hostile work environment occurs when there is discriminatory conduct or behavior in the place of work that is unwelcome and offensive to an employee or group of employees based on a protected class status. Harassment can be based on one's gender, age and/or race.



The church is subject to liability for what it knows or should have known. If an employee complains of harassment within the context of his/her employment, the church is likely to be found to have had knowledge. Under some circumstances, if an employee fails to report an incident, the court may deem that the church should have known of the harassment.

A church is required to take action to stop the harassment of its employees. The action should be reasonably calculated to end the harassment. In other words, the church should put forth the effort of any reasonable employer. What makes corrective action reasonable depends on the facts in the circumstances. In the case we mentioned earlier, the harassment continued for three years after the employee reported the behavior. The court found that to be unreasonable.

This case is a warning for churches that have employees. You must ensure that your employees have a harassment-free work environment. At the very least, you should have policies that address this matter. Beyond that, your church should provide training for your staff on what to do if they find harassment in your workplace. Taking preventive steps today may help your church avoid civil liability later. ■

Churches Face Data Breach Risks

Recent events in the news illustrate the damage a data breach can cause to an organization. Churches are subject to many of the same risks that plague most businesses. One type of risk is the threat that unauthorized persons will gain access to private information. I raise this issue because this is a real risk that should have the attention of church leaders. Further, there are corporate governance implications for not taking prudent actions.

Most churches have private information in their possession. Some of the confidential information includes business records on internal operations. Other information includes files on dealings with church members. These files may include personal, private information not otherwise available to the public.

Members share a variety of non-public information with their church. Confidential information includes financial records, health and medical disclosures, employment needs and family matters. Church members probably rely on the church's ability to safeguard the confidentiality of these files.

Church management should review its policies and procedures for the protection of confidential records. These guidelines should take into account the various ways a data breach can take place at the church. Unauthorized data loss can occur with online files as well as physical records.

Some churches rely on Internet or local computer files for their official records. With technology, churches can be at risk of electronic data breaches. Data breaches can lead to public embarrassment, legal liabilities and loss of membership.

There is an operational cost to online or offline data breaches. Operational costs increase when church staff has to react, repair and respond to the public when there has been a data security incident. The Ponemon Institute released a study in May 2013 that looked at the costs associated with data breaches. The study provided the average cost to a business for a data breach is $188 per record. Leaders may consider this number times the number of members to get a sense of how costly it could be to their church.

Electronic data breaches can occur though the malicious acts of outsiders. Outside intrusions include attacks by hackers and software viruses. Electronic breaches can also stem from the action of insiders. Staff and volunteers can mistakenly release confidential data to outsiders when duped by emails and other forms of communications.

Church management should develop policies and procedures to address their exposure to data breach risks. The policy should guide the church's position on processes and approaches. The church policies should provide standards on how it will provide notifications to members if a breach happens. The procedures provide a framework for how the church will respond and recover.

Churches may be able to mitigate the cost of a data breach with insurance. Churches that have liability insurance should talk with their providers. Some policies include provisions that cover data breaches. Just as important, the insurance policy may defend the church should a data breach lead to a legal action for damages.

The best defense for data breaches is to take precautions that avoid a loss in the first place. If the unthinkable happens, a church will be able to rebound faster if it has effective plans and procedures. ■

Legal Counsel for Churches is a service provided by M Smith Law, PLLC for members of the religious community. This periodical is intended to help churches and their officials become better prepared to address important legal and governance issues. We hope you find *Legal Counsel for Churches* a valuable resource. For each issue, we try to raise relevant issues and offer some practical alternatives. We welcome your comments and input.

Post Office Box 27461, Raleigh, North Carolina 27611 919.362.0744 (*voice*) 888-321.9047 (*fax*) maurice.smith@msmithlaw.us