CARR MALONEY PC

LEGALLY SPEAKING

Carr Maloney PC is a litigation firm providing comprehensive legal services throughout the mid-Atlantic region. Businesses and individuals use the firm as a single resource to meet all of their legal needs. Recognizing that each client's legal issue comes with its own specific complexities, **we simplify the complex.**

June 2015

In this issue:

Courts are Split on Whether Websites Must be ADA Accessible

By: Thomas L. McCally, Esq. and Matthew D. Berkowitz, Esq.

The Americans with Disabilities Act ("ADA") provides that "[n]o individual shall be discriminated against on the basis of disability in the full and equal enjoyment of the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation by any person who owns, leases (or leases to), or operates a place of public accommodation." 42 U.S.C. § 12182.

Although a website is not included in the definition of "public accommodation" under § 12181(7), claimants, including those with visual and hearing impairments covered under the ADA, have argued that a website is a "place of public accommodation" under the ADA, and thus, a website must be ADA compliant. Courts are split as to whether website is covered by the ADA. Some courts have held that the ADA does not apply to websites, especially when there is not a sufficient nexus between the virtual discrimination alleged and a physical place.

For example, recently, the Ninth Circuit Court of Appeals in *Cullen v. Netflix*, No. 13-15092 (9th Cir. April 1, 2015), and in *Earll v. eBAY, Inc.*, No. 13-15134 (9th Cir. April 1, 2015), held that that Netflix and eBay were not subject to the ADA because their website services were not connected to any "actual physical place." These rulings were based upon a prior Ninth Circuit decision, which held that the ADA applies only to businesses that have a connection to a place where they offer goods and services. *See Weyer v. Twentieth Century Fox Film Corp.*, 198 F. 3d 1104, 1114 (9th Cir. 2000).

The decisions of the Ninth Circuit are in conflict with other recent decisions, including one equally recent decision out of a district court in the First Circuit. In *National Federation of the Blind v. Scribd Inc.,* No. 2:14-cv-162, 2015 WL 1263337 (D. Vt. March 19, 2015), the Court held that a digital library's website and mobile application were places of public accommodation under Title III of the ADA. In reaching its conclusion, the Court noted that the First, Second, and Seventh Circuits have indicated that Title III applies even in the absence of some connection to a physical place. The *Scribd* Court also noted that Netflix lost on the same issue in the District Court of Massachusetts. In *Nat'l Ass'n of the Deaf v. Netflix*, *Inc.*, the Court ruled that the ADA "applies with equal force to services purchased over the Internet." 869 F. Supp. 2d 196, 200 (D. Mass. 2012).

Given the split in decisions, it is only a matter of time before the Supreme Court is tasked with deciding whether a website is a place of public accommodation under the ADA. Further advancing the notion that the ADA may cover both the virtual as well as the physical is the anticipated release of Department of Justice's ("DOJ") long awaited website accessibility rules. The rules, if ever enacted and which were expected to be released earlier in 2015 but are now expected in 2016, could address new standards and obligations of businesses to make websites ADA compliant. The general consensus, though, is that websites, in the near future, will be considered a "place of public accommodation" under the ADA.

In the meantime, the DOJ has brought enforcement actions against notable U.S. companies. For example, in 2012, the DOJ filed a Statement of Interest against Netflix for failing to caption streaming video, asserting that the lack of captioning violated the ADA. And last year, following enforcement actions, the DOJ entered into settlement agreement with Ahold U.S.A., Inc. and Peapod, LLC, regarding the accessibility of www.peapod.com and its associated mobile application. The DOJ also recently entered into and with H&R Block. The consent decree with H&R Block requires it to comply with Web Content Guidelines (WGAC) 2.0, which the DOJ has recognized as the "international industry standards for web accessibility.

Additionally, a number of U.S. companies have entered into structured settlement agreements with private plaintiffs, following civil suits. These companies, which include Major League Baseball and Bank of America, have agreed to ensure that their websites comply with WCAG 2.0. Thus, whether regulations are in place or not, there will likely be an increase in lawsuits against businesses demanding that their websites become accessible to all.

One Less Thing to Worry About at the M & A Closing: Maryland, D.C., and Virginia Offer Viable Defenses to Baseless Derivative Shareholder Lawsuits

By: Thomas L. McCally, Esq. and Matthew D. Berkowitz, Esq.

On the heels of the recent financial crises, there has been a significant increase in the number of derivative shareholder lawsuits filed against corporations, including a corporation's officers and directors. Often, these suits arise during the pendency of one company's purchase of another company. The crux of the suits is that the directors of the to-be acquired company breached their fiduciary duties to the to-be acquired company and its shareholders. The suits also generally allege that the purchasing company and to-be acquired company aided and abetted the officers and directors' purported breaches.

Because a derivative lawsuit is filed by shareholders on behalf of the corporation and recovery belongs to the corporation, plaintiff's attorneys often file the lawsuit contemporaneously with, or jointly as, a class action shareholder lawsuit. As such, shareholders may be entitled to recovery and attorneys' fees may be awarded. In many instances, such a suit is nothing more than a strike suit, whereby a meritless lawsuit is filed with the purpose of effectuating a quick settlement that might be less than defense costs and attorneys' fees that could be awarded. The defendant corporation also may have a motivation to settle quickly so as not to delay or destroy the pending deal closing. Additionally, these suits are often filed in state court (with no chance of removal) to take advantage of typically lower pleading standards and sometimes more plaintiff friendly juries.

Although plaintiffs' attorneys and litigious shareholders may initially have leverage because of the costs involved in defending such a suit and the threat that it poses to the pending deal, the targeted corporations have a number of defenses available, many of which are procedural in nature, that serve to quickly and favorably defeat the suit and save the deal. The following are some early procedural defenses that are available in Maryland, the District of Columbia and Virginia:

A Genuine and Legitimate Pre-Suit Demand is Required

All three local jurisdictions – Maryland, the District of Columbia, and Virginia – hold that a derivative claim may be barred unless the plaintiff first makes a pre-suit demand.

In Maryland, before commencing a derivative action, the plaintiff generally must make a pre-suit demand to the corporation's board of directors, unless such demand would be "futile."[1] The Court may dismiss the complaint on a motion to dismiss on the grounds that no pre-suit demand was made and it is apparent from the face of the complaint that the plaintiff cannot satisfy the futility exception. For the futility exception to apply, "the allegations or evidence [must] clearly demonstrate, in a very particular manner, either that (1) a demand, or a delay in awaiting a response to a demand would cause irreparable harm to the corporation, or (2) a majority of the directors are so personally and directly conflicted or committed to the decision in dispute that they cannot reasonably be expected to respond to a demand in good faith and within the ambit of the business judgment rule."[2]

Similarly, in the District of Columbia, under Superior Court Rule of Civil Procedure 23.1, a shareholder bringing a derivative action must plead either (1) that he has made a demand for action upon the corporation's directors which the directors wrongfully refused, or (2) that the demand would have been futile because, for example, the majority of directors have a conflict of interest or failed to validity exercise their business judgment.[3]

In Virginia, a shareholder-plaintiff in a shareholder derivative suit must make a pre-suit demand pursuant to Va. Code § 13.1-672.1.[4] In determining whether the demand is sufficient, the Court will consider (1) whether the demand adequately identifies the alleged wrong; (2) whether the demand letter adequately demands action on the part of the corporation or its officers to redress the alleged wrong; (3) whether the demands are clear and particular enough to have put the corporation on notice as to the substance of the alleged wrong and allow the corporation assess its rights and obligations with respect to the alleged wrong; and (4) whether the alleged wrong and claims asserted in the plaintiff's complaint are sufficiently connected.[5]

Indeed, in all three local jurisdictions, dismissal of a shareholder derivative suit may be occur at the initial pleading stage if no pre-suit demand was made or if the demand itself, or the related allegations, are insufficient.

---

[1] *See Werbowsky v. Collomb*, 362 Md. 581, 620-21 (2001).

[2] *Id.* at 620.

[3] *Behradrezaee v. Dashtara*, 910 A.2d 349, 357 (D.C. 2006) (citation omitted).

[4] Va. Code § 13.1-672.1.B. provides:

No shareholder may commence a derivative proceeding until:

1. A written demand has been made on the corporation to take suitable action; and

2. Ninety days have expired from the date delivery of the demand was made unless (i) the shareholder has been notified before the expiration of 90 days that the demand has been rejected by the corporation or (ii) irreparable injury to the corporation would result by waiting until the end of the 90-day period.

[5] *Williams v. Stevens*, No. CL12-4830, 86 Va. Cir. Ct, 2013 WL 8118657, at *4-6 (April 1, 2013) (granting plea in bar in part because the demand letter failed to seek a particular redress of a particular wrong).

The Business Judgment Rule Further Guards Against Meritless Claims

Relatedly, all three jurisdictions recognize the business judgment rule to protect claims against directors. In Maryland, the business judgment rule (which is codified in Maryland Code, § 405.1 of the Corporations and Associations Article) heavily presumes that a corporation's director has (1) acted in good faith; (2) in a manner that he reasonably believes to be in the best interests of the corporation; and (3) with the care than an ordinarily prudent person in a like person in a like position would use under similar circumstances.[6] The rule precludes judicial review of legitimate business decisions, absent a showing of fraud, bad faith, self-interest or gross negligence.[7]

Similarly, in the District of Columbia, a director gets the presumption of the business judgment rule unless plaintiff can show that the director acted in manner that was inconsistent with the corporation's business purpose, acted in bad faith, or was grossly negligent.[8] In Virginia, a director is shielded from liability if the director acted in good faith and in best interests of the corporation.[9] As is the case with respect to pre-suit demands, a shareholder suit may be subject to dismissal if the pleading fails to sufficiently allege facts to overcome the business judgment rule.[10]

Other Early Defenses Are Available

Furthermore, the local jurisdictions, particularly Maryland, provide additional mechanisms that allow for an early disposal of a shareholder holder suit. For example, in Maryland and to the extent that the suit is a direct shareholder action (i.e., a class action lawsuit), § 405.1 of the Corporations and Associations Article bars direct mismanagement claims against directors of a corporation, unless it is for decisions made outside the purely managerial context, such as negotiating the price shareholders will receive in a purely cash-out merger transaction.[11]

Additionally, the typical breach of fiduciary duty claims against the directors may be barred because Maryland does not recognize breach of fiduciary duty as a separate cause of action.[12] Although some Maryland courts have allowed the breach of fiduciary claims to proceed forward (or dismissed the suit on other grounds) in the derivative shareholder suit context,[13] other Maryland Courts have steadfastly ruled that such breach of fiduciary duty

[6] *See Boland v. Boland*, 423 Md. 296, 328-331 (2011) (citing Md. Code § 405.1).
[7] *See Black v. Fox Hills North Community Ass'n*, *Inc.*, 90 Md. App. 75, 82 (1992).
[8] *See Behradrezaee*, 910 A.2d at 361-62.
[9] *See Simmons v. Miller*, 261 Va. 561, 576-77 (2001) (citing Va. Code § 13.1-690).
[10] *See, e.g., Werbowsky*, 362 Md. at 622; *see also Strubb v. Cole Holdings Corp.*, Case No. 24-13-001563, Circuit Court for Baltimore City (2013).
[11] *Shenker v. Laureate Education*, *Inc.*, 411 Md. 317 (2009).
[12] *Wasserman v. Kay*, 197 Md. App. 586, 631-32 (2011) (citing cases).
[13] *Shenker*, 411 Md. at 346.

claims fail as a matter of law.[14] And because a breach of fiduciary duty claim against the directors fails, so must the typical intertwined aiding and abetting claim.[15]

With respect to the District of Columbia, Superior Court Rule of Civil Procedure Rule 23.1, like its federal equivalent, requires a heightened pleading standard in derivative actions by shareholders. For example, the pre-suit demand under Rule 23.1 requires that [t]he complaint . . . allege with particularity the efforts, if any made by the plaintiff to obtain the action the plaintiff desires from the directors . . . and the reasons for the plaintiff's failure to obtain the action or for not making the efforts." Rule 23.1 also states that a "derivative action may not be maintained if it appears that the plaintiff does not fairly and adequately represent the interests of the shareholders . . . ."

Summary

In light of the foregoing defenses, defendant directors and merging corporations may find success in filing a motion to dismiss, especially when the shareholder derivative suit is nothing more than a strike suit. If nothing else, an early dispositive motion often highlights the meritless nature or the weakness of the plaintiff-shareholder's claims. Moreover, in instances where the action is truly a baseless strike suit, sending plaintiff's counsel a "Rule 11" or a "Frivolous Lawsuit" letter prior to filing a motion to dismiss may be prove to be successful. In some instances, the plaintiff and his attorney will appreciate that the corporate defendants are not going to pay the ransom and will agree dismiss the suit to avoid potential sanctions or to avoid the cost of a losing fight.

A derivative shareholder suit may initially pose significant risks and costs to the directors and merging companies, but with favorable facts and when defended properly, the suit may ultimately turn out to be just a hiccup towards a successful closing.

Virginia Supreme Court Addresses Foreseeability, Collectibility and Emotional Distress Damages in Legal Malpractice Cases

By: Dennis J. Quinn, Esq. and Kristine M. Ellison, Esq.

On February 26, 2015, the Virginia Supreme Court reversed a jury verdict against a Fairfax County attorney and provided new guidance on multiple issues that commonly arise in legal malpractice litigation. In Shevlin Smith v. McLaughlin, the Court addressed three questions that were previously unanswered or at least somewhat unclear. In short, the Court held: 1) that an attorney does not breach a duty to his client by failing to correctly foresee a judicial ruling on an unsettled legal issue; 2) that collectibility is relevant when the alleged

[14] *Gorby v. Weiner*, C.A. No. TDC-13-3276, 2014 WL 4825962, at *11 (D. Md. Sept. 23, 2014); *Kay*, 197 Md. App. at 631-32.
[15] *See Kay*, 197 Md. App. at 632; *Gorby*, 2014 WL 4825962, at *16.

injury in a legal malpractice claim is the loss of an otherwise viable claim; and 3) that non-pecuniary damages are not recoverable in a legal malpractice claim.

This decision involved a complex set of facts and procedural history as the plaintiff, McLaughlin, brought a legal malpractice claim against an attorney who had represented him in a prior legal malpractice suit.

On foreseeability, the attorney argued that he did not breach his duty as a matter of law when he failed to correctly predict the Supreme Court's ruling on the application of the joint tortfeasor statute to legal malpractice defendants. Although the Court had previously ruled as a matter of law that an attorney does not breach his duty when he follows "well-established law" that is later reversed, the Court had not squarely addressed this related issue. Declining to adopt the brightline judgmental immunity/attorney judgment rule, the Court held: "[I]f an attorney exercises a 'reasonable degree of care, skill, and dispatch' while acting in an unsettled area of the law [at the time of the alleged breach] . . . then, the attorney does not breach the duty owed to the client."

On collectibility, the attorney challenged the $5.75 million jury verdict for the former client, contending that this amount was more than what he could have collected in the first legal malpractice action had the attorney not been negligent. The Court agreed with the attorney, holding that collectibility is relevant to a legal malpractice plaintiff's damages. And taking it one step further, the Court determined that because collectibility is not an element of a plaintiff's prima facie case for legal malpractice, noncollectibility of a lost claim is an affirmative defense that an attorney must plead and prove.

The former client's cross-appeal raised the issue of recovery for pain and suffering and wrongful incarceration allegedly resulting from the attorney's malpractice. In response, the Court followed its prior decisions categorizing legal malpractice claims as breach of contract claims and applying Virginia's economic loss rule. If it wasn't clear before, this decision makes it clear now: "'tort damages' – including non-pecuniary damages such as mental anguish, emotional distress, and humiliation – 'are not recoverable'" in legal malpractice claims in Virginia.

A Business Owner's Guide to Preparing for and Responding to Data Breach Incidents

By: Nat P. Calamis, Esq. and J. Peter Glaws, Esq.

With the dramatic increase of data breach incidents over the past several years,[16] it has become increasingly important for businesses to understand their responsibilities in

[16] See IBM Security Services 2014Cyber Security Intelligence Index, April 2014. Available at http://www-935.ibm.com/services/us/en/it-services/security-services/data-breach/.

protecting sensitive data within their control, as well as the risks associated with failing to do so. This is particularly true for small and medium sized businesses, which could face potentially catastrophic consequences resulting from a data breach incident. The purpose of this article is to give a general overview of proactive steps that businesses can take to protect themselves from the consequences of data breach incidents, as well as steps that businesses should take in the event that a data breach incident occurs.

1. Make Sure That You Have Appropriate Insurance Coverage In Place

Many of the major insurance carriers are currently writing specifically designated cyber liability insurance policies that provide various types of coverage in the event of a data breach incident. This could include coverage for: business interruption, costs of computer forensic vendors to assist with responding to a data breach; and, 3rd party claims resulting from a breach. It is important to note that there have been cases where courts have determined that insurance carriers are not responsible for providing coverage for data breach incidents under a commercial general liability insurance policy. *See, e.g. Zurich American Ins. Co. v. Sony Corp.*, Case No. 651982 (N.Y. 2011). Therefore, understanding exactly what type of insurance coverage your business has in place is critically important.

If your business does not currently have cyber liability insurance coverage, you should consider talking to your insurance broker about the risks associated with your particular line of work and whether you should purchase a cyber-liability policy.

2. Determine Whether There Are Regulations Or Guidelines That Govern The Protection Of Sensitive Data Within Your Industry

There is currently no comprehensive federal legislation setting forth specific guidelines for the protection of data. As a result, businesses are left with a patchwork of state and federal laws and regulations, many of which are industry specific, and some of which may or may not be binding upon a particular business.

A few federal examples include: the Health Insurance Portability and Accountability Act of 1996 (HIPAA) that requires HIPAA covered entities to comply with privacy and security rules; the Gramm-Leach-Bliley Act of 1999 (GLB) that regulates the management of personal information in the hands of companies that are significantly engaged in financial activities; the Family Education Rights and Privacy Act of 1974 (FERPA) that regulates disclosure of personal information in the hands of education institutions that receive federal funds (as well as their partners and vendors); Section 5 of the Federal Trade Commission Act, that gives the Federal Trade Commission prosecutorial authority over businesses that violate consumers' privacy rights, or mislead them by failing to maintain security for sensitive consumer information; and, among others, the Commerce Department's National Institute of Standards and Technology (NIST) framework on improving critical infrastructure cybersecurity for the nation's financial, energy, health care and other industries with critical electronic systems.[17]

[17] Although not a binding law, the NIST framework sets a bar for compliance with other cybersecurity laws and regulations.

It is important for businesses to fully understand the type of data that is within their possession (i.e. medical records, social security numbers, credit card information), and to have an understanding of which statutes and guidelines are in place that govern the protection of that data.

3. Have Data Response Procedures In Place

When a data breach incident occurs, a rapid response is imperative. Many statutes and regulations have reporting requirements with fairly immediate deadlines, and penalties can be assessed if these deadlines are not adhered to. In addition, businesses can face liability exposure for failing to take reasonable steps in responding to data breach incidents. As a result, it is important for businesses to have policies in place *before* a data breach incident occurs to ensure a quick and efficient response. Businesses should designate an individual to be the point person in responding to a data breach incident. This individual should be responsible for managing and coordinating the roles of various third parties that will need to be contacted to provide assistance in the event of a data breach, and for reporting to the various stakeholders within the organization. At a minimum, a business should have a written policy designating the point person within the organization for data breach responses, and providing a list of third parties that should be contacted immediately in the event of a data breach. The list of third parties should include legal counsel, the insurance broker, a computer forensics vendor and a public relations firm, if necessary.

Actions to Take in Response to a Data Breach

In addition to taking proactive measures to try to prevent data breach incidents, businesses need to be aware of the affirmative steps that need to be taken in the event that a data breach incident occurs. A September 2014 Ponemon Institute survey of 567 executives in the United States resulted in a staggering 43 percent of respondents reporting that they had experienced data breach incidents within the past year.[18] There has been a sharp increase in malicious, intentional attacks on businesses by hackers and other cyber criminals in recent years.[19] So even if businesses take reasonable measures to prevent data breach incidents, it is still quite possible that these incidents can, and will, occur. Below is a list of actions that should be taken if and when a business learns of a data breach incident.

1. Find The Source of the Breach and Correct The Problem

Finding the source of a breach or potential breach and fixing the problem can be a difficult task that requires assistance from outside computer forensic consultants or even law enforcement. It is important to note that when the source is discovered, significant damage may have already taken place as a substantial number of data breach incidents go undetected for long periods of time. For example, in 2014, the U.S. Department of Homeland Security's Computer Emergency Readiness Team issued an advisory on newly detected

[18] "Is Your Company Ready for a Bid Data Breach?" The Second Annual Study on Data Breach Preparedness, Ponemon Institute Research Report, sponsored by Experian Data Breach Resolution, September 2014.
[19] See IBM Security Services 2014Cyber Security Intelligence Index, April 2014. Available at http://www-935.ibm.com/services/us/en/it-services/security-services/data-breach/.

"Backoff" malware affecting Point of Sale systems.[20] At the time of the advisory, however, the malware was largely undetectable by then current anti-virus systems. Thus, affected businesses likely did not know of an ongoing breach until implementation of the recommended upgrades to their cybersecurity software.

Because of the likelihood of existing damage at the time a breach or suspected breach is discovered, it is important to have outside legal counsel involved from the moment an organization suspects a breach. Participation by outside counsel in the organization's communications with computer forensic vendors will help to preserve and protect the attorney-client privilege, to the extent possible.

2. Determine Your Responsibilities Pursuant to State Data Breach Notification Laws

Almost every state and the District of Columbia currently have their own separate data breach notification laws on the books. While many of these state notification laws are quite similar, there are important differences that make the process of responding to a data breach incident impacting sensitive data of residents spread out over many states extremely tedious, time consuming and expensive. It is important for businesses to hire competent legal counsel immediately after learning of an actual or suspected data breach incident to provide guidance and advice regarding the organization's responsibilities pursuant to state notification laws. If the business has purchased cyber liability insurance coverage, it is possible that this insurance policy will pay for legal counsel.

3. Determine Your Responsibilities Pursuant to Industry-Specific Laws/Regulations

In addition to state notification laws, businesses also need to be aware of industry-specific guidelines and regulations that could govern the response to a data breach incident. The examples noted above, including, among others, HIPAA, GLB, and FERPA place specific requirements on entities with notice that personal information within their control has been compromised. It is important for business to determine what industry-specific guidelines or regulations may be implicated in the event of a given data breach incident.

Conclusion

Recent events clearly suggest that data breach incidents are going to become more and more common in the immediate future. It is, therefore, crucial for businesses of all sizes to take steps to try to minimize their exposure to these types of incidents.

[20] U.S. Dept. Homeland Security Alert TA14-212A, August 17, 2014. Available at https://www.us-cert.gov/ncas/alerts/TA14-212A

Is Your Dress Code Policy Discriminating?

By: Tracy D. Scott, Esq.

Employers of all kinds require dress codes for their employees. In fact, uniforms are standard in the retail and hospitality industry from employers attempting to not only reflect a polished, professional appearance, but also seeking brand recognition. In recent years, however, many employers have been sued by employees for dress codes that employees allege infringe upon their religious beliefs.

In the recent opinion of *EEOC v. Abercrombie & Fitch*, the Supreme Court, decided 8 to 1 against Abercrombie & Fitch and ruled that the company's dress code that prohibited headwear violated civil rights laws. Abercrombie maintains a strict dress code or "look policy," which details what its employees are allowed to wear, and not wear, at work. In the case of Samantha Elauf, the retailer's ban involving a hijab, a headscarf worn by some Muslim women, was found discriminatory.

Samantha Elauf, a Muslim teenager, sued the retailer after being denied a position at a Tulsa, Oklahoma store. Testimony from the store's manager revealed that Ms. Elauf was denied a position based on her wearing a black hijab at her interview. According to the brief submitted by the EEOC, Ms. Elauf scored high enough at her interview with the interviewing manager to be hired. However, because the "look policy" bars employees from wearing caps and black clothing at work, the interviewing manager consulted with the store's district manager about Ms. Elauf's hijab. After speaking with the district manager, the interviewing manager stated that the district manager directed her to lower Ms. Elauf's interview score and to recommend that the applicant not be hired.

Abercrombie & Fitch argued that they should not be held liable for religious discrimination because Ms. Elauf never specifically revealed in her interview that she wore the headscarf for religious reasons and, to have assumed that she did so for religious reasons, would have been requiring the retailer to treat applicants differently based on stereotypes. Ms. Elauf's position and that of the EEOC, which brought the suit on her behalf, was that she should not have been required to make a specific request for a religious accommodation to wear a hijab at her interview. "How could she ask for something when she didn't know the employer had such a rule?" Justice Ginsburg said during the February oral arguments. In writing for the majority, Justice Scalia stated that "[a]n employer who has actual knowledge of the need for an accommodation does not violate Title VII by refusing to hire an applicant if avoiding that accommodation is not his *motive*. Conversely, an employer who acts with the motive of avoiding accommodation may violate Title VII even if he has no more than an unsubstantiated suspicion that accommodation would be needed."

Title VII of the Civil Rights Act of 1964 prohibits employers from discriminating against individuals because of their religion in hiring, firing, or any other terms and conditions of employment. Title VII also requires employers to reasonably accommodate the religious beliefs and practices of applicants and employees, unless doing so would cause an undue burden on the operation of the employer's business. Whether a particular accommodation

would pose an undue burden on the employer's business depends on individual circumstances and may relate to among other things, cost, safety, or efficiency.

Abercrombie & Fitch is not the only company that has been sued for allegations of religious intolerance. In 2014, Mims Distributing Company in Raleigh, North Carolina settled a claim filed by the EEOC for $50,000 on behalf of Charles Alston. Mr. Alston, a Rastafarian, applied for a job as a delivery driver for Mims. During his interview, he was told that he would be hired if he agreed to cut off his dreadlocks. Mr. Alston advised that as a practicing Rastafarian, it was against his religious beliefs to cut his dreadlocks and that he would not do so. He was denied the position. As part of its settlement agreement with the EEOC, Mims also agreed to create an official religious accommodations policy, to conduct trainings annually on Title VII policies, and post a copy of its anti-discrimination policy at its Raleigh facility.

Inconsistently applied dress codes, or an employer's failure to provide reasonable accommodation for such dress codes can give rise to discrimination claims under Title VII. Employers need to have well-written policies in place. Additionally, employers must make sure that policies are explained to managers and are applied uniformly. If employers are considering implementing or revising their dress code policies, attorneys at Carr Maloney, PC are well-versed in employment law and can provide guidance on this and other employment law issues.