PERSPECTIVES

SCHERER SMITH & KENNY LLP
THE STRENGTH OF PARTNERSHIP

140 Geary Street, Seventh Floor ▪ San Francisco, CA 94108-4635
Phone: (415) 433-1099 ▪ Fax: (415) 433-9434 ▪ www.sfcounsel.com

November 2016

Scherer Smith & Kenny LLP serves mid-sized and fast-growing entrepreneurial companies. From complex litigation to business, real estate, intellectual property and employment law, our team brings strategic thinking, pragmatism and intense dedication to our clients' success.

"Perceived" Disabilities Under California's Fair Employment and Housing Act

California's Fair Employment and Housing Act ("FEHA") provides ample protections to employees against discrimination in the workplace. Once such protection is found at California Government Code section 12940(m), which requires that employers make a "reasonable accommodation" for an employee's known disability. The recent California Court of Appeal Case of *Moore v. Regents of the University of California* (2016) 248 Cal.App.4th 2016 demonstrates how broad this obligation is and how aware employers must be of their obligations under FEHA.

In *Moore*, the plaintiff, Deborah Moore, was employed as the Director of Marketing for the University of California, San Diego. During her employment, Moore developed a heart condition that required she wear a "life vest," which was a type of external defibrillator. Upon coming to work in the vest, Moore stated that "there was nothing to worry about," that her condition "would take care of itself," and "I'm fine, seriously." Moore stopped wearing the vest after only a few weeks. Moore's supervisor, Kimberly Kennedy, commented that UCSD needed to "lighten your load to get rid of some of the stress." Kennedy later disclosed to Moore that she considered her "a liability to the department." Moore's employment was eventually terminated as part of an alleged downsizing, and Moore later filed suit against the University of California. One of the several claims she asserted was a violation of California Government Code section 12940(m) claiming that the University failed to offer her a reasonable accommodation.

At trial, the court found against Moore on the basis that "she did not have a disability that required accommodation." However, the Court of Appeal reversed this finding. In doing so it noted that while actual disabilities are protected, FEHA also protects employees who are perceived as or regarded as having a disability. In this case, Kennedy's comments evidenced Moore's employer regarded her as being disabled, which the court found to be sufficient under FEHA to sustain Moore's claim for failure to accommodate.

Moore is critical for California employers to understand as it highlights the need to carefully handle situations involving employees who disclose

In This Issue

Denis Kenny

Fall is in the air. The Holidays are right around the corner. By the time you read this, Halloween will have passed but you will undoubtedly remember that Halloween fell on most of our least favorite days: Monday. Ugh. Talk about a rude reminder that Halloween is not a *true* holiday! My heart

need to carefully handle situations involving employees who disclose medical conditions or communicate work restrictions. Such conditions do not need to amount to an actual disability. Indeed, in a case such as *Moore*, the employee could expressly deny he or she has a disability multiple times, but such communications could nevertheless fail to alleviate an employer's obligation to engage in the interactive process to determine if a reasonable accommodation is available for the employee. Further, as FEHA provides a more expansive definition of "disability" than does federal law and the law of most other states, California employers need to be aware of an even more extensive list of possible conditions and circumstances that could give rise to failure to accommodate claims. Consequently, employers must be constantly aware of communications such as those at issue in *Moore* and be prepared to respond appropriately throughout the potential interactive process that an employer must engage in with a disabled employee.

We at Scherer Smith & Kenny LLP remain available to assist you with any employment-related or other legal issues. Please contact Denis Kenny (dsk@sfcounsel.com), Ryan Stahl (rws@sfcounsel.com), or John Lough (jbl@sfcounsel.com) for more information.

-Written by Ryan Stahl

Preparing for the Worst: A Data Breach

It is an unfortunate fact of our current word but cyber breaches are in the news almost every day now. Many companies either have or will suffer a cyber-attack at some point. It may seem inevitable but there are steps you can take to prevent or at least minimize the damage from a breach, as well as prepare for how to respond if it does happen.

Preparing for a cyber breach really consists of two parts. The first is what to do before you suffer a breach. The second is what to do after you suffer a breach despite your best efforts to prevent one from occurring. We discuss both of these below.

Steps to Take to Prevent or Minimize the Damage of a Breach:

Nearly everyone hosts data in some fashion these days. Whether the data is credit card information for payments, customer contact information or critical data necessary for you to perform your business, many of our clients are holding data that needs to be protected. Some hold that data on-site while others store it in the cloud with a service such as Amazon Web Services. How and where you hold it is up to you but, regardless, you need to be proactive in making sure the data is secure. Damages, fines, penalties and costs associated with a breach, depending on its severity, can be hundreds of thousands, if not millions of dollars. So it pays to invest in doing what you can to protect against a breach.

This can take many forms but below are some of the key ways you can prepare:

1. Make sure your computer systems are secure and protected against an intrusion and that you have thoroughly vetted any third parties that are hosting data of yours (including credit card information, personal information of customers, health care information etc.). Once the system is set up and secure you should consider an audit of it to make sure you have followed the right protocols and that any third party you hired to help with the test set it up correctly.

2. Look at your contracts and especially your Business Associate Agreements ("BAA") if those are applicable for your business and make sure your liability in the event of a breach is limited (if possible) to something you can live with or your insurance limits.

3. Appoint someone at your organization to be the key point person to handle a breach and to coordinate efforts preparing for and responding to a breach.

bleeds for teachers forced to endure the Tuesday after Halloween with kids fully depleted of their sugar fueled vigor. Nonetheless, Halloween has become one of my favorite days in the Holiday season.

You might wonder why I am so fond of Halloween. Or, perhaps, you don't care. Either way, I will explain. Halloween is special because it creates memories and instills a spirit of unconditional giving.

First, the memories. Whether or not you have children, we can all remember what it felt like to be a child on Halloween. I still remember many of my childhood costumes. I raided my father's closet most years coming up with last minute (and frantically put together) costumes. I swear my Dad kept every stitch of clothing he got when serving a tour of duty in Vietnam as a Captain in the Army. I loved wearing his jungle camouflage gear and packing a knife for authenticity purposes only (could you imagine that being allowed in today's world?). My dad's closet also provided ample gear for the nerd costume. Remember, Revenge of the Nerds? My father held onto what he called "timeless" clothes. As a teenager in the 50's, he had an assortment of short-sleeved, button-down, plaid shirts (buttoned to the top for

responding to a breach.

4. Review your insurance and upgrade as necessary. Insurance takes many forms but it can literally save your business if you have the right type in place.

    a. Most business have (or should have) a commercial general liability policy ("CGL"). This coverage may also extend to personal and advertising injuries. It is very unpredictable as to whether this traditional insurance policy will cover damages associated with a breach such as forensic work, PR firms, notification costs, credit monitoring costs etc. and courts interpret these policies very differently.
    b. There are other types of insurance that some businesses have such as fidelity/crime, director and officer insurance, and business interruption coverage. These policies are hit or miss and may not cover all the damages and cost you face in the event of a breach.
    c. The most thorough coverage is cyber liability insurance that specifically covers damages from a cyber breach. However, the types of policies offered differ widely and there is not yet an industry standard here so you should make sure to go over the coverage under each policy. Here are some common costs to ask about:

        i. Hiring a PR firm
        ii. Notifying customers of the breach
        iii. Hiring forensic experts who may be needed to investigate the breach in your computer system
        iv. Whether it covers a breach of a third party hosting your data (i.e. the breach was not of your system but of a third party but you suffer damages as a result)
        v. Credit monitoring costs
        vi. Fines and penalties, including legal fees

These expenses can be high so make sure to get as much coverage as needed, which is often $2-5 million.

<u>If you do Unfortunately Suffer a Breach here are Some Steps to Take Immediately:</u>

1. First, and we cannot emphasize this enough, immediately notify your insurance company regardless of the type of policy you have in place. Anything you spend before notifying your insurance company, such as hiring a PR and law firm to help manage the immediate fallout and notification likely won't be covered by your insurance if you do it before you notify them. If you hire a PR firm and a law firm and spend $100,000 the first week and thereafter notify your insurance company it is very common for these initial costs to not be covered. A final benefit is that your insurance company is probably dealing with a breach on a daily basis, so they will have referrals to attorneys and PR firms, who can help you immediately.

2. Immediately notify your core team and make sure no one communicates anything to the outside (customers, press etc.) without approval by the CEO or other officer in charge. You need a consistent message that is not rushed.

3. Immediately work out a plan with your PR firm and attorneys to manage the damage, if any, and to determine if you need to notify the authorities or not.

4. Take steps to stop further intrusions by figuring out how the breach occurred and then fixing it.

5. Take notes on everything you find. Memories fade and having an accurate record of what went down, who said what etc. is key since

(buttoned to the top for instant nerd attire) and peg legged pants (which, when shortened, made perfect "floods"). White socks, black shoes, tape-rimmed glasses with coke bottle lenses (courtesy of my grandfather with glaucoma) and wet-gelled hair parted in the middle, completed my standard nerd costume attire.

I trust these memories will trigger some from each of your lives. One thing is certain: Halloween is meant for fun, laughs and smiles; no grouches allowed.

At the heart of Halloween is the spirit of unconditional giving. It is a perfect opportunity to host a casual party. For those with children, setting up your home as an open house and base for your neighbors and friends to stop by for appetizers and libations before, during or after trick or treating, is convenient and easy fun. For several years we were *that* family and our party included a haunted house which spanned our entire basement. I spent days setting up the haunted house and tried to increase the spookiness with each passing year. Many a child ran from the room within seconds of entry. That was a sure sign of success.

Whether you host a party, walk with your young ones around the neighborhood trick or treating, adorn your

you'll likely be asked later by clients, your insurer, possible buyers of your company etc. for details around the breach and trying to remember names, dates, order of events etc. a year later is very difficult (especially if the person who handled the breach has left

6. Comply with all notification or alerts required in your contracts. Many contracts or BAAs, as well as laws such as HIPAAA require very quick notice to the affected parties or that you at least alert them to the fact that a breach has occured. This time period can be very short (24-48 hours).

This is a complicated area but with some preparation now before something happens you can reduce or prevent a breach from occurring and if disaster does strike you'll be better prepared to respond quickly and appropriately. We at Scherer Smith & Kenny LLP remain available to assist you with any corporate or or other legal issues. Please contact Brandon D. Smith (bds@sfcounsel.com) or Heather Sapp (hgs@sfcounsel.com) for more information.

-Written by Brandon Smith

Avoiding Independent Contractor Misclassification

I have written many articles and frequently speak at seminars and webinars concerning the increasingly widely-publicized legal arena known as independent contractor/1099 ("IC") misclassification. IC misclassification is the moniker used to describe the situation when a hiring party (an individual or a business) erroneously treats a worker (an individual or a business) as an IC instead of an employee. The legal ramifications of IC misclassification are immense and include damages (e.g., unpaid wages, meal and rest period premiums, and healthcare and retirement plan/401k benefits), penalties (e.g., payroll taxes, prejudgment interest) and attorneys' fees and costs, among other expenses.

The U.S. Department of Labor (the "DOL") has recently attempted to educate the public about avoiding IC misclassification. These education efforts include the August 2016 issuance of a publication entitled Misclassification Mythbusters, which cites twelve "myths' which the DOL explains are commonly cited by hiring parties and workers alike as reasons for IC classification. The DOL proceeds to correct and educate the public by providing the real "facts" concerning each of these myths.
See https://www.dol.gov/whd/workers/Misclassification/myths.htm

Misclassification Mythbusters follows by just over one year the July 2015 issuance of an Interpretation by the Administrator of the DOL Wage and Hour Division dealing with IC misclassification (the "Interpretation"). https://www.dol.gov/whd/workers/misclassification/ai-2015_1.htm. The Interpretation is a much more comprehensive and, many would say, convoluted treatise covering a number of areas in addition to IC misclassification including a focus on the prevalence of "exempt" employee misclassification. The usefulness of the Interpretation as an educational tool has also been widely questioned as its content seems more appropriate for an audience of experienced employment law attorneys and scholars than the general business public. Nonetheless, the DOL's decision to issue, within just one year, two IC misclassification-specific publications, highlights the critical import of IC misclassification in our current legal landscape. Whenever the government attempts to explain its laws, the public should be concerned. The IC misclassification legal arena provides a fitting reason to be concerned.

treating, adorn your home with an array of spooky decorations, buy loads of treats to leave outside your door or simply stay home and open your door to welcome the children with laughs and smiles at all the unique, timeless and timely costumes, one theme is consistent. Halloween is about making memories fueled by unconditional gifts (and aided by sugar-filled candy, of course).

I encourage us all to apply the attributes of Halloween to the rest of our Holiday season and our daily lives. I know that is easier said than done, but recognizing the greatness of what defines Halloween is at least a step in the right direction.

- *Written by Denis Sullivan Kenny*

A fundamental lesson evident from the current IC misclassification legal arena is: proceed with utmost care before retaining any IC. Instead of following the DOL's path of trying to understand and apply the various "myths" and "facts" surrounding IC misclassification, I suggest you accept the following assumption for any hiring decision: a worker will be considered your employee unless you can prove otherwise, not vice versa.

Start by asking yourself the following discrete questions: am I (1) hiring an outside business (2) to perform a discrete, specialized task or set of tasks (3) which I am not otherwise able or which may not be suitable for my existing staff to handle in-house? If your answers to any of these three basic questions is, no, you better not choose IC classification. If your answers are primarily, yes, then you ***may*** be on the right track toward viable IC classification ***but*** you still need to consider a number of other factors before making a definitive decision.

Examining and explaining the application of the various IC/employee factors, indicia and tests which differ (sometimes widely) from agency to agency and jurisdiction to jurisdiction is outside the scope of this brief article. Suffice to say, one test definitely does not fit all. This reality, again, demonstrates the importance of consulting with trusted counsel before diving into the potential pitfalls of IC engagement and misclassification.

We at Scherer Smith & Kenny LLP remain available to assist you with any employment-related or other legal issues. Please contact Denis Kenny (dsk@sfcounsel.com), Ryan Stahl (rws@sfcounsel.com), or John Lough (jbl@sfcounsel.com) for more information.

-Written by Denis Kenny

Areas of Practice

Business; Real Estate; Intellectual Property and Employment Law; Litigation and Dispute Resolution; Nonprofit; Estates and Trusts

For more information: www.sfcounsel.com