THE BKCG BULLETIN

Winter 2015 Edition

BKCG
BURKHALTER KESSLER CLEMENT & GEORGE LLP

Holiday Stress? California's Fair Employment and Housing Act May Not Cover Your Work-Related Stress Claims

California's Fair Employment and Housing Act ("FEHA") prohibits an employer from discriminating or otherwise retaliating against its employees based upon a qualifying medical disability. FEHA-protected disabilities generally include any mental or physical condition that "limits a major life activity" of the employee. Work is considered a "major life activity" under FEHA.

With this background in mind, any medical condition that in some measurable way "limits" or makes difficult an employee's job duties is arguably protected under FEHA. The California legislature and courts have specifically recognized certain conditions as protected disabilities under FEHA, including autism, clinical depression, HIV, and hepatitis, to name a few. If an employee is unable to perform the functions of her job because of such a disability, the employer must then engage in a good faith interactive process with the employee and provide a reasonable accommodation to enable the employee to maintain employment, unless such accommodation creates an "undue hardship" to the operation of the employer's business. Accommodations often include a reduced or "light" workload or reduced hours.

The limits on FEHA-recognized disabilities were recently put to the test in the May 2015 case of *Higgins-Williams v. Sutter Medical Foundation, 237 Cal.App.4th 78 ("Higgins")*. In *Higgins*, plaintiff was a clinical assistant for defendant Sutter Medical Foundation ("Sutter"). Plaintiff worked under two particular supervisors for approximately three years before reporting to her physician complaints of work-related stress directly linked to her supervisors. Plaintiff's physician diagnosed plaintiff as having adjustment disorder with anxiety, and reported plaintiff's disabling condition as "stress when dealing with her Human Resources and her manager." As a result, plaintiff then took approximately six months of stress-related leave from her employment. Plaintiff's physician advised Sutter that plaintiff could only return to work on a light duty schedule to a different department, though did not provide Sutter any information on a reasonable accommodation that would allow plaintiff to return to her position as a clinical assistant. In other words, plaintiff was only cleared to return to work under different supervisors. After plaintiff and her physician failed to timely provide Sutter with any information as to plaintiff's return to her clinical assistant position, Sutter terminated plaintiff's employment.

Plaintiff brought FEHA-related claims for disability discrimination and retaliation against Sutter which claims were summarily adjudicated against plaintiff. The Court of Appeal affirmed the decision in favor of Sutter on the grounds that plaintiff did not establish she had a qualifying disability under FEHA. The Court specifically ruled: "[A]n employee's inability to work under a particular supervisor because of anxiety and stress related to the supervisor's standard oversight of the employee's job performance does not constitute a mental disability under FEHA." The Court in *Higgins* relied upon the ruling in the 1999 case of *Hobson v. Raychem Corp.*, where there Court similarly reasoned that courts interpreting FEHA, "have uniformly declined to extend protection to persons whose alleged disabilities rendered them unable to perform a particular job even though they might have been physically able to work in a different position."

Although the Court's ruling in *Higgins* is based upon a specific set of facts, *Higgins* demonstrates that there are limits to the protection afforded employees under FEHA for work-related stress.

Please contact Amber M. Sanchez at (949) 975-7500 or asanchez@bkcglaw.com if you have questions about any issue discussed in this article, or any other related matter.

Does the State Have Your Money?

Many of us have accounts we haven't checked up on in a while: savings accounts we started for a specific goal that we've since put on hold; dividend reinvestment accounts we started to finance a child's higher education. We probably assume that these accounts will be there when we need them. Because of a practice called escheat, however, that assumption could end up turning your financial life upside down.

Escheat laws were originally intended to create a sort of giant "lost and found" for each state. Unclaimed property could be taken away from institutions that might try to hide them on their books and hope that no one noticed they were gone. But to cover budget shortfalls, some states quietly empty this lost and found into their general funds, trampling private property rights in the process.

So how does an investment account or other property get confiscated as unclaimed property?

Accounts become "abandoned" in a number of ways. You can fail to cash a check, forget to update the address on the account, fail to respond to a proxy statement or simply fail to make contact with your financial institution for a defined period of time. That can range anywhere between just three and seven years.

Once an asset reaches the "abandoned" threshold, the institution may try to contact you via mail or phone before reporting your property as unclaimed. But if the owner's address is wrong or he or she simply doesn't open the letter, the escheat process begins.

States find out about abandoned accounts in one of two ways: your financial institutions could include it in a required yearly filing or it could be discovered in an audit.

Before taking possession of the property, most state laws require an attempt to find and contact the owner. If the owner isn't found or doesn't come forward, the property is transferred to the state. Physical property or securities are either held as is or converted to cash through sale or auction. Depending on state law, the resulting cash may be transferred directly into the state's general fund to close budget gaps or simply held in case the owner comes for it.

How do you avoid escheat?

- Keep your address up to date with all financial institutions and employer.
- Cash all checks.
- Open all mail from financial institutions.
- Keep a list of all accounts and account numbers.

If you eventually discover what happened and want to get your property back, you have to make a claim on it and fill out paperwork to prove your identity.

(continued on page 4)

In This Issue

5 Things You Should Be Aware of Regarding Data Security Breaches

Hardly a month goes by without another high profile, embarrassing data security breach being publicized, whether it is the theft of millions of Target customers' credit card information, or the publication of senior Sony executives' extremely embarrassing internal e-mails. For purposes of this article, we will define "data" very broadly, as everything from a company's personnel information to customer information (credit card details, SSN, driver's license, account numbers) to confidential and proprietary company information (financial information, customer lists, R&D work, new product details, etc).

How does that affect me, you may ask? Well, according to a recent Pew Research Center survey, 43% of U.S. firms had experienced some form of data breach in the prior year. What's more, data breaches can hit everyone from small businesses to multi-billion dollar conglomerates, with equally devastating effects. In fact, smaller businesses generally offer easier pickings than larger companies, because they are less security-conscious and do not have the rigorous internal security-related policies and resources (such as in-house IT staff) that larger firms do. This article focuses on 5 basic things that every business needs to be aware of, both to prevent a data breach and to minimize the effects of a data breach, if one does occur.

1. Employee error and malfeasance is the main cause of data breaches and not hackers. Depending on what survey you believe, only perhaps 20% of all data breaches result from overt hacking. The other 80% are due to a combination of employee negligence, malicious employee activity (such as a departing employee taking customer trade secret information with her), lax data protection procedures and employees' unsafe use of mobile devices to access companies' networks. So, while it obviously makes sense to educate and train employees to engage in sound e-mail practices to avoid computer viruses and malware, it is even more important to focus on other more fundamental data breach risks. This includes both the mundane (such as shredding important company documents before throwing them out) to limiting access to confidential information to employees with a need to know (rather than having all company documents and data on a company server which is accessible to a large number of employees), to regularly changing computer and network passwords.

2. Understand your business' specific legal obligations in advance of a breach. A wide array of state and Federal laws may apply to your business in the event of a data security breach. For example, California law requires any business to notify a California resident whose unencrypted personal information[1] was acquired, or reasonably believed to have been acquired, by an unauthorized person. California Civil Code §1798.82(a). The law also requires that a sample copy of a breach notice sent to more than 500 California residents must be provided to the California Attorney General. As another example, for healthcare providers, the Federal HIPAA statute governs individually identifiable health information, the unauthorized disclosure of which triggers its own set of breach notification requirements. Find out before a data security breach occurs at your company exactly what data disclosure laws you are subject to, what you would be required to do in the event of a data security breach, who you are required to notify and when. Failure to comply with the applicable requirements for your industry and business could result in significant fines and unwanted regulatory scrutiny, not to mention a class action lawsuit.

3. Examine your own internal company policies. Since employees and contractors are responsible for the majority of data security breaches, such an internal examination is crucial. This can encompass everything from conducting criminal background (and, where permissible, credit) checks on prospective employees, having internal financial checks and balances (since good old-fashioned employee embezzlement is still very much alive and well!), to carefully managing what data is divulged to vendors and under what circumstances, to requiring your vendors and business partners to demonstrate their ability to safeguard your data, so-called vendor credentialing (the business of one of BKCG's current clients). Another safeguard to consider is the implementation of what is known as a BYOD ("Bring Your Own Device") policy, to regulate how employees are permitted to access and use your company's e-mail server and computer network using their own mobile devices (or even wearable technology, such as Google Glass), a virtually ubiquitous business practice nowadays. The fact that an employee uses his or her own laptop, tablet or smartphone for company business in no way restricts an employer's ability to set restrictions (or outright prohibitions) on how or whether that device can be used to access, use, store and transmit company data. Remember, a chain is only as strong as its weakest link and one stolen employee laptop that is not encrypted, or which lacks adequate security measures, can cost a company millions of dollars! As examples, a well-written BYOD policy should include limitations on the range of acceptable employee devices; give the employer the explicit right to remotely wipe the employee's device (which may include the employee's personal data), if the device is lost or stolen, upon termination of employment or in the event of a data breach; or even search the device, under certain specified circumstances.

4. Data security breaches can be very costly. Don't be a cheapskate with your preventive and anticipatory measures! Stop and consider, for a moment, how much it would actually cost your business in lost revenue, disgruntled ex-customers, legal fees to defend a class action, regulatory agency fines and investigations and destruction of company goodwill if your company was crippled by a serious data breach - for example, the hijacking of your entire computer network for a week, the theft of all your customers' credit card information, or the disclosure, to your fiercest competitor, of your sales and marketing plans for your revolutionary new product line? Now consider what resources you have dedicated, to date, to preventing or mitigating a data security breach that could cause such problems. Do you have sufficient of the right types of business insurance, such as cyber risk and fidelity/crime insurance, to help cover the cost of such a loss? Do you have an Employee Handbook, and matching, consistently enforced employee policies that adequately address employee confidentiality and data security issues? Have you engaged a qualified and competent IT company to assess and address potential vulnerabilities in your company's computer systems, equipment and practices to data breaches before they can be exploited? If your answer to any of these questions is "No", it's time to act! Cutting corners on such prudent steps could be a catastrophically illusory cost-saving measure for your company.

5. Have a recovery plan in place. Whether you company creates a formal "Security Incident Response Team" or not, you should have a well-thought out and widely-disseminated recovery plan in place, clearly laying out how you will respond if and when a data security breach befalls you. Who will do what and when, especially in the crucial first few hours after the breach is discovered? Is your data safely backed up and accessible if you cannot use your computer network to conduct business for an extended period of time? Do you have access to an IT resource who can immediately help you assess what happened, prevent further breaches and take swift and appropriate remedial action? And, of course, do you have legal counsel who can properly advise you on and help you address your legal obligations and potential legal risks resulting from a data security breach? The time to be asking yourself these questions is NOW, and not for the first time, after a data security breach that could cripple your business has already occurred. As with all things in business, hope for the best, but be prepared for the worst!

[1]"Personal information" is very broadly defined by this statute as any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.

Please contact Greg Clement at (949) 975-7500 or gclement@bkcglaw.com if you have questions about any issue discussed in this article, or any other aspect of business law.

Will the Whistle Blow on DFS?

If you have watched any college or pro football games this fall, chances are you have been deluged with TV advertisements for DraftKings and FanDuel, the leaders in the exploding daily fantasy sports ("DFS") industry. For years, DFS providers managed to stay under the radar, but a recent scandal has placed them – and the DFS industry as a whole – in the crosshairs of federal and state lawmakers.

The troubles for DFS arose out of rumors that a single DraftKings employee had used information unavailable to other DFS participants to turn a $25 entry fee on FanDuel into a $350,000 prize. As a result, many jurisdictions are reconsidering whether DFS constitutes illegal gambling, and the legal ramifications are widespread and intimidating.

In Florida, the U.S. Attorney is investigating whether DFS operators violated the Illegal Gambling Business Act of 1970 ("IGBA"). This law, which was passed with mafia-funded gambling operations in mind, carries potential penalties that include imprisonment, forfeiture of profits and assets and fines. A federal grand jury has been impaneled to review evidence and testimony related to relevant targets, including DFS companies in Florida. If the grand jury finds probable cause, meaning it is more likely than not that a crime occurred, indictments could issue against the employees of DFS companies. The Justice Department and the FBI also have expanded their respective inquiries, to include possible RICO violations, regarding the legality of fantasy sports into ones that focus specifically on DFS.

In addition to the criminal investigations, many civil lawsuits already have been filed against DraftKings and FanDuel in federal district courts since the scandal broke, with more likely to follow. These lawsuits all aspire to be class action lawsuits contending that FanDuel and DraftKings deceived consumers through advertisements and public assurances into believing that they can win at DFS by being "smarter than the average fan." The plaintiffs allege that winning at DFS is not based on skill, but rather on being the beneficiary of a fixed game where DFS employees have access to information unavailable to other DFS participants. The named plaintiff in one such action has alleged that he started winning at DFS once DraftKings and FanDuel announced that they were no longer allowing employees to play the other companies' DFS games. If true, this allegation suggests that alleged insider trading had a meaningful impact on probability of winning.

As with all lawsuits, the process will be slow and arduous and will involve many issues that our clients endure in their own litigation. DraftKings and FanDuel likely will file motions to dismiss these lawsuits and attempt to enforce arbitration clauses in their on-line, click-through terms of service. If the DFS lawsuits advance past motions to dismiss, federal judges would then turn their attention to whether to certify the lawsuits as class actions. Class certification is a complex process that itself takes months and sometimes years. In assessing certification, judges would determine if the plaintiff in the lawsuits adequately represent other DFS participants. It is also possible that multiple DFS lawsuits could be consolidated into one larger case (as has occurred in recent sports litigations, including the concussion lawsuits brought by retired NFL players).

Pretrial discovery also will be an extremely sensitive and important issue. Plaintiffs will demand the product of computer data, gaming algorithms, security protocols and emails that will invoke issues of privacy, confidentiality, trade secrets, and a multitude of other public relations woes and legal problems.

Recently, the Nevada Gaming Control Board ruled that DFS counts as a form of sports betting under Nevada law. While the classification of DFS as gambling does not make it automatically unlawful in Nevada, it means that DFS companies will need to apply and obtain a license from the Nevada Gaming Control Board in order to lawfully operate in Nevada. In the meantime, DFS will essentially be banned in Nevada, with criminal sanctions a possibility for DFS companies who ignore the ban. While the interests of DFS companies and traditional gaming companies are often not aligned since they are, to some extent, competing industries, the two operate in the basic arena, and a gaming company would obviously rather you place a bet in Nevada than play a DFS game in Nevada. Given that gambling companies exert significant political influence in Nevada, the state's ban of DFS could be politically motivated.

Moreover, Nevada's decision could have wide-reaching impact of other states follow its lead as other states may defer to Nevada's determination of what counts as "gambling." For example, the Illinois Gaming Board concluded that DFS appears to be illegal under Illinois law, and the Attorneys General of both New York and Massachusetts have expressed their doubts about the lawfulness of DFS under their states' laws.

DFS has also caught Congress's eye, and it could soon revisit the legal framework for sports betting and DFS, as existing laws could be modified to dramatically change how sports betting companies and DFS companies conduct business in the United States. If Congress schedules hearings on sports betting and DFS, lobbyists would play a pivotal and well-financed role in shaping those hearings. The gaming and DFS industries would have a great deal of money to spend on those lobbyists and an even greater deal of money to lose or gain if Congress tries to change the law.

DFS's rise in popularity over the past few years has been staggering, and it is anybody's guess whether its fall will be as precipitous and severe. In view of the troubling allegations of insider trading by the employees of the two industry leaders, however, for now, the only way to win may be not to play at all.

Please contact Michael Oberbeck at (949) 975-7500 or moberbeck@bkcglaw.com if you have questions about any issue discussed in this article, or any other related matter.

THE NEW YEAR BRINGS NEW LAWS

ESTATE TAXES

Under the most recent legislation governing federal estate taxes, the amount of wealth that an individual may transfer to his or her heirs tax free, the exemption amount, was set at $5,000,000 in 2010. The exemption amount increases every year with inflation. The exemption amount for 2015 was $5,430,000. Due to mild inflation, the exemption amount will increase only slightly to $5,450,000 in 2016. Remember that for married couples, the amount doubles to $10,900,000 if proper steps are taken. The annual gift exclusion remains at $14,000 per person.

TRANSFER ON DEATH DEED

Effective January 1, 2016, California will now allow a property owner to execute a Revocable Transfer On Death Deed. This law allows an individual to sign a deed to his or her property wherein the deed names a beneficiary who will receive the property upon the owner's death. This deed must be recorded within 60 days of signing and may be revoked at any time by signing and recording a new deed.

This type of deed is only available for property with 1 - 4 residential dwellings, a condominium, or agricultural land of 40 acres or less improved with a single family dwelling. This law sunsets on December 31, 2020. It is our opinion that these types of deeds should be avoided as we feel they will cause more problems than they will solve. We wanted to make you aware of the law and encourage you not to use it.

END OF LIFE ACT

Also beginning January 1, 2016, terminally ill individuals who meet specified requirements may request and self-administer life ending drugs. This law sunsets and is no longer in effect on January 1, 2026. In order to be able to avail yourself of this law you must meet the following criteria:

- Must be an adult in California with a terminal disease.
- Must have the capacity to make medical decisions.
- Must have been given a prognosis of less than 6 months to live.

The patient must request an aid-in-dying drug from his or her physician. The patient must also have the ability to self-administer the drug. No assistance with the ingestion of the drug is permitted. There are other requirements and restrictions and we are sure more regulations will be handed down as the law is utilized in the coming years.

Please contact William George at (805) 373-1500 or at wgeorge@bkcglaw.com if you have questions about any issue discussed in this article.

DOES THE STATE HAVE YOUR MONEY?

(continued from page 1)

The state would then return your property if it was still in their possession, or if it was sold, cut you a check for the proceeds of the sale, even if that amount is significantly less than appraised or current market value.

So how can consumers protect their property from escheatment?

The best way is to stay in contact with whoever is holding your property, be it a financial institution, bank or employer. Keeping your address up to date, cashing dividend checks and opening all your mail from these institutions can insure your name won't come up on an auditor's ledger.

Keeping a list of all your accounts with the names of the institutions and account numbers in case you pass away unexpectedly is also recommended. That way, you can be sure your property will go to your heirs and not an aggressive state auditor.

Claiming Unclaimed Property in California

In California, property is generally presumed abandoned if it has remained unclaimed by the owner for more than three years after it became payable or distributable. However, this time limit varies depending on the type of property involved. Once abandoned property is turned over to the state by a business, an individual then generally has five years to reclaim.

No sale of escheated property may be made until 18 months after the final date for filing the report. Securities listed on an established stock exchange and other securities may be sold by the Controller no sooner than 18 months, but no later than 20 months, after the final date for filing the report.

Any property delivered to the Controller that has no apparent commercial value must be retained by the Controller for a period of not less than 18 months from the date the property is delivered to the Controller.

In any case, unclaimed property held by the state may still be found by searching the state's website at http://www.sco.ca.gov/col/ucp/

To find out if other states may be holding your unclaimed property, search the national database established by the National Association of Unclaimed Property Administrators (NAUPA).

A claim for recovery of abandoned property is filed with the State Controller on a form designated by that agency. The Controller must investigate the claim and render a decision within 180 days. The agency must notify the claimant by mail of its decision.

Claims denied or not decided by the Controller within 180 days after the claim was filed may be appealed by filing an action naming the State Controller as defendant in the superior court of any county or city in which the California Attorney General has an office. The action must be brought within 90 days of the Controller's decision or within 90 days after the deadline for the Controller's decision.

Please contact Camille Vasquez at (949) 975-7500 or at cvasquez@bkcglaw.com if you have questions about any issue discussed in this article.

The BKCG Bulletin is Published By:

Burkhalter Kessler Clement & George LLP

2020 Main Street
Suite 600
Irvine, CA 92614
Attn: Alton G. Burkhalter
949.975.7500
949.975.7501 fax
www.bkcglaw.com

340 North Westlake Blvd.
Suite 110
Westlake Village, CA 91362
Attn: William C. George
805.373.1500
805.373.1503 fax

BKCG

Visit our new web site at www.bkcglaw.com

Be sure to visit us on LinkedIn

Burkhalter Kessler Clement & George LLP (BKCG) advises and protects businesses and high net worth individuals through experienced litigation and transactional lawyers. Core practice areas include: Business litigation in state and federal courts, as well as FINRA, AAA and JAMS arbitration and mediation; Corporate, transactional and employment law documentation; and Estate Planning and Probate services through the Firm's State Bar certified Estate Planning Specialist.