EPSTEIN BECKER GREEN

TECHNOLOGY, MEDIA & TELECOMMUNICATIONS

Your Workplace. Our Business.®

EMPLOYMENT LAW DESK REFERENCE

In the lifecycle of a start-up, there are many key issues, situations and milestones when it is important to seek consultation. Refer to this document regularly and consider contacting an Epstein Becker Green employment, employee benefits or immigration lawyer if:

ONBOARDING AND COMPENSATION

- You are considering hiring your first employee.
- You are posting a job description.
- You are hiring an individual with an existing non-compete from another employer.
- You want to hire a non-citizen.
- You are hiring an intern.
- You are hiring an independent contractor or freelancer.
- You are preparing to enter into stock-option and deferred compensation arrangements.
- You are paying someone solely with deferred compensation or stock options.
- You have independent contractors performing the same job function as W-2 employees.
- You want to offer healthcare coverage for your workforce.

MANAGING EXISTING WORKFORCE

- You have a long-time independent contractor.
- You learn that an employee wants to take a leave of absence of any kind.
- You receive a phone call, letter or any other document from an attorney, court, or government agency.
- You want to protect yourself against an employee who may be in a position to take your ideas and go work for a competitor.
- You are not sure whether a person is entitled to overtime compensation.
- You are concerned about an employee's performance or behavior.
- You are contacted by a union seeking to represent your employees.

SEPARATION

- You are preparing to terminate an employee for performance.
- You wish to terminate an employment or consultancy agreement.
- You have a worker that is leaving and who is trying to steal your clients, your talent or your ideas to go work for a competitor or themselves.
- You are considering paying an employee severance.
- You receive a "lawyer's letter" from an attorney representing a former employee.
- A former employee files for State Unemployment Benefits and you receive notice of same.
- You plan to merge, buy, sell or close your business.

It is Also Important to Know the Thresholds for Coverage Under Several Key Statutes – Triggered by Employee Count

EMPLOYEE COUNT	STATUTE APPLICABLE
0-3 employees	» Fair Labor Standards Act ("FLSA") – Establishes minimum wage, overtime pay and related requirements. » New York State Wage and Hour Law – Establishes minimum wage, overtime pay, worker misclassification and related requirements. » New York State Labor Law – Establishes minimum wage as well as regulations concerning hours of work, payment of wages, deductions from wages and related requirements. » New York City Earned Sick Time Act – Establishes requirements for providing employees with unpaid sick time policies that comply with the statute's requirements (Once you have 5 employees, must provide paid sick leave). » California Labor Code and Industrial Welfare Commission Wage Orders - Specifies wages, hours and working conditions including minimum wage, overtime pay and meal/rest break requirements, and provides recordkeeping requirements for personnel and payroll records. » California Wage Theft Prevention Act – Requires employers to provide notice to new hires of information pertaining to wages and sick leave entitlements. » California Fair Employment and Housing Act ("FEHA") – Prohibits harassment and requires employers to take reasonable steps to prevent harassment and investigate harassment claims. » California Healthy Workplaces, Healthy Families Act (effective July 1, 2015) – Establishes minimum paid sick leave requirements for employees who work more than 30 days in California during their first year of employment. » California Kin Care Law (Labor Code 233) – Entitles an employee to use up to one-half of his or her annual paid sick leave to attend to the care of a family member (as defined by the statute).
4 or more employees	» All of the above statutes, plus: » New York State Human Rights Law – Prohibits discrimination in employment based on age, creed, race, color, sex, sexual orientation, national origin, marital status, domestic violence victim status, disability, military status, arrest record, conviction record, and predisposing genetic characteristics. » New York City Human Rights Law – Prohibits employment discrimination in hiring, firing, and work assignments; salary; benefits; promotions; performance evaluations; and discipline on the basis of actual or perceived age, race, creed, color, national origin, gender, disability, marital status, partnership status, sexual orientation or alienage or citizenship status of any person.
5 or more employees	» All of the above statutes, plus: » New York City Earned Sick Time Act – Establishes requirements for providing employees with paid sick time policies that comply with the statute's requirements. » California FEHA – Requires equal employment opportunities and provides protection against discrimination or retaliation in employment because of age, ancestry, color, race, religious creed (including religious dress and grooming practices), disability (mental and physical) including HIV and AIDS, marital status, medical condition (cancer and genetic characteristics), genetic information, military and veteran status, national origin (including language use restrictions), race, sex (which includes pregnancy, childbirth, breastfeeding and medical conditions related to pregnancy, childbirth or breastfeeding), gender, gender identity, and gender expression and sexual orientation. » California Pregnancy Disability Leave Act - provides up to four months of unpaid leave to employees who are disabled due to pregnancy, childbirth or related medical conditions.
15 or more employees	» All of the above statutes, plus: » Title VII of the Civil Rights Act ("Title VII") – Prohibits discrimination in hiring, promotion, discharge, pay, fringe benefits, job training, classification, referral, and other aspects of employment, on the basis of race, color, religion, sex or national origin. » Americans with Disabilities Act ("ADA") – Requires engaging in process to provide disabled employee with a reasonable accommodation and prohibits discriminating against qualified individuals with disabilities in job application procedures, hiring, firing, advancement, compensation, job training, and other terms, conditions, and privileges of employment.
20 or more employees	» All of the above statutes, plus: » Age Discrimination in Employment – Prohibits discrimination against people who are age 40 or older. » Continuation of health coverage under the Consolidated Omnibus Budget Reconciliation Act ("COBRA") (consider also State mini-COBRA laws for lower thresholds)
50 or more employees	» All of the above statutes, plus: » Family Medical Leave Act ("FMLA") – Provides certain employees with up to 12 weeks of unpaid, job-protected leave per year. It also requires that their group health benefits be maintained during the leave. » California Family Medical Leave Act – Provides similar benefits to California employees as the FMLA with some key distinctions, including coverage for registered domestic partners. » California FEHA – Employers must provide at least two hours of anti-harassment training to supervisors every two years. » Affordable Care Act ("ACA" / "Obamacare") –Requires employers with 50 or more full-time (including full-time equivalent) employees to offer compliant healthcare coverage to its full-time employees and their dependents or subject to shared responsibility payments.

July 16, 2015

Five Technology, Media, and Telecommunications Developments Important to Employers

---

For the latest employment, labor and workforce management news and insights in the technology, media, and telecommunications industry, subscribe to our Technology Employment Law blog.

The laws that govern the workplace affect companies in the technology, media, and telecommunications industry in myriad ways. From the rise in workplace discrimination claims unique to this industry and the increase in union organizing activities affecting high-tech and new media companies, to Federal Trade Commission ("FTC") regulation of social media policies, compliance in the workplace is a challenge. Further, as new technologies are introduced into the workplace, additional hurdles arise, including data privacy and security obligations as well as policies on working with robots and robotic systems that are compliant with Occupational Safety and Health Administration ("OSHA") recommendations. This issue of Epstein Becker Green's *Take 5* addresses all of these evolving issues confronting employers:

1. **BYOD Programs: Privacy and Security Issues and Minimizing the Risk**
2. **High Tech and New Media: Organized Labor's New Frontier**
3. **A Growing Role for the FTC in Regulating Workforce Management**
4. **Avoiding Age Discrimination Complaints in an Industry Noted for a Lack of Age Diversity**
5. **Robotics in the Workplace: How to Keep Employees Safe and Limit Exposure to OSHA Citations**

1. **BYOD Programs: Privacy and Security Issues and Minimizing the Risk**
   By Brandon C. Ge

As mobile devices become more prevalent, employers are increasingly turning to bring-your-own-device ("BYOD") programs that allow employees to use their personal devices for work purposes. More people are beginning to own multiple mobile devices, such as smartphones and tablets, and wish to use these devices for work purposes. Even without an employer-sanctioned BYOD program, many employees choose to use their personal devices for business purposes, allowing them to work from nearly anywhere.

A BYOD program can provide several benefits. Employees—who often develop preferences toward particular devices or brands—can use whatever devices they prefer. Instead of having to acclimate to company-issued devices, employees can use devices with which they are already familiar. Many people also find it inconvenient to carry company-issued devices in addition to their personal devices when traveling. With the growing emphasis on lighter and thinner mobile devices, many employees are reluctant to neutralize these weight savings by carrying extra devices. Companies may also find that they save money by not having to issue devices and manage data and voice plans. These savings can instead be used to provide support and maintenance.

While BYOD programs have potential benefits for both companies and employees, many companies struggle to design programs that maintain these benefits while protecting the privacy and security of sensitive data. Depending on the organization, such data may include individuals' personal, financial, and health data, as well as important business-related data, such as human resources information, confidential information related to legal matters, and trade secrets. Therefore, employers need to consider various measures to minimize the risk involved in a BYOD program.

Concerns for Employers

By allowing employees to use their own devices for work purposes, employers lose some degree of control compared to a company-owned device. Although criminal cyberattacks frequently make headlines, employee negligence and lost or stolen devices continue to be a primary cause of data breaches. People tend to carry their personal devices everywhere, so when they are allowed to create, store, and transmit work-related information on these devices, there is a heightened risk of exposing sensitive company data to unauthorized individuals when these devices are lost or stolen.

There are also risks that do not involve loss or theft of devices. For example, if employees download malicious software, third parties may gain access to sensitive data. As another example, employees, especially those who own multiple devices, often store or back up their data in the cloud for convenient access across devices. In this instance, if the cloud service provider experiences a security breach, the company's information may be at risk.

Employers also need to keep in mind that people frequently allow friends and family to use their personal devices. Compounding the risk is that when devices are shared with trusted friends and family members, the devices are often handed off already unlocked, potentially allowing unrestricted access to company information and networks. Friends and family members may also lack the employee's security training and may inadvertently install malicious software that puts company data at risk.

Companies must consider business purposes, such as preserving reputation, as well as the numerous potential legal obligations surrounding data privacy and security. For example, federal and state breach notification laws would apply to the unauthorized use or disclosure of certain types of data. The information may be subject to many confidentiality laws, such as the Health Insurance Portability and Accountability Act ("HIPAA") Privacy Rule. Businesses need to consider the various security laws that may apply, such as the HIPAA Security Rule and the Gramm Leach Bliley Act. There may be contractual obligations or trade secret laws to keep in mind. Employment laws may also enter the picture. For example, if nonexempt employees are allowed remote access via their BYOD devices, they might perform more "off the clock" work, which could give rise to wage and hour claims.

Moreover, employees may have privacy concerns. While some enjoy the freedom to use personal devices for both work and personal reasons, others may be hesitant to blur the lines between their work and personal lives. Some employees may be concerned about the privacy of their personal data, such as photos, text messages, personal email, and web browsing histories.

Implementing a Successful BYOD Program

One of the first steps in implementing a BYOD program is determining which employees should be permitted to participate. Not everyone in an organization needs mobile access to work e-mail and files. Certain positions in the organization may also involve greater risk that outweighs the benefits of participation. Employers should carefully analyze the various job functions within the organization and determine whether participation in the BYOD program is appropriate for each.

To address the concerns associated with a BYOD program, employers should have a carefully crafted BYOD policy and make sure that employees read, understand, and consent to its terms and conditions. The terms and conditions should describe the ways in which the employer will access and use employees' devices. For example, employers should retain the right to access devices for business purposes, if necessary. The policy should also describe employees' responsibilities, which may include reporting lost or stolen devices within a certain timeframe and refraining from using unapproved devices or installing unapproved applications.

Businesses should adopt procedures that address termination of employment, including procedures for deleting company data stored on terminated employees' devices.

Processes should be implemented to ensure that terminated employees no longer have access to company networks.

Companies should also implement various technical safeguards, such as encryption and passcode protection. Using a mobile device management ("MDM") solution can help with configuring and enforcing these safeguards. MDM software can allow employers to require encryption and strong passwords, disable cloud services, lock devices after a period of inactivity, remotely wipe lost or stolen devices, and prevent the installation of unapproved applications on employees' devices. MDM solutions can also help companies track which devices are participating in the BYOD program.

Training is vital to a successful BYOD program. Training should include regular reminders of good security practices, such as using strong passcodes, physically securing devices against loss or theft, and refraining from giving others access to devices that are used for work. BYOD programs shift much of the control over security to employees, so it is vital that employees are properly trained and receive periodic training refreshers.

2. High Tech and New Media: Organized Labor's New Frontier

By Steven M. Swirsky

When one thinks of industries where union activity remains strong and additional organizing is likely, one may think of health care, education, retail, heavy manufacturing, and other "old school" fields, but not high tech and "new media." Recent developments, however, including targeted campaigns focusing on employers in the Silicon Valley, its East Coast cohort Silicon Alley, and online, demonstrate that these assumptions may not be correct. High tech and new media are in the sights of not only some of America's most actively organizing unions but also a coalition of interest and advocacy groups that are partnering with a coalition of unions with the common goal of increasing union representation at high-tech companies and the various contractors, subcontractors, and vendors that clean their facilities, feed their employees, and drive them to and from their facilities.

Taken together with the recent rule changes adopted by the National Labor Relations Board ("NLRB" or "Board") to allow for much faster union representation elections in smaller units defined by unions, and the Board's continuing emphasis on the application of the National Labor Relations Act to employees who are not represented by unions and who work in non-union workplaces, employers in the high-tech and new media fields should be aware of how these forces can impact their businesses and the ability to maintain dynamic workplaces.

Silicon Valley Rising: An Industry-Targeted Movement

When 1930s legendary bank robber Willie Sutton was asked why he robbed banks, he replied that was where the money was. Today's labor unions, with their emphasis on income inequality and the gap between the 1 percent and the 99 percent have realized

that Silicon Valley and technology companies are where the money is today and that there are many more employees in these industries who are not receiving the high salaries, stock options, and perks that many think of when they think of Silicon Valley.

A well-financed effort by a coalition of unions—including the Teamsters, the Service Employees International Union (SEIU), the Communication Workers of America (CWA), UNITE-HERE, the South Bay Labor Council, the NAACP, and other community organizations—have banded together to establish "Silicon Valley Rising" to organize employees of high-tech employers and the various vendors and service providers that they rely upon.

Silicon Valley Rising' describes its goal as addressing what it sees as a two-tiered economic system in which, in its view, direct employees of the companies in the technology and media industry are paid well and receive good benefits, while those who support the industry as employees of contractors and suppliers are not. Silicon Valley Rising's focus includes the vendors and contractors that Silicon Valley employers rely upon for transportation, maintenance, food service, and the like.

One of Silicon Valley Rising's first successes came earlier this year, when it was certified as the bargaining representative of the company that Facebook relies upon to provide shuttle bus services between its various facilities at its headquarters. Soon after it won a representation election, Teamsters Local 853 negotiated a first contract with Loop Transportation that significantly increased wages and benefits and changed work rules and the like. In its campaign, Local 853 made clear that it saw the party that ultimately controlled the purse strings as being Facebook and media reports demonstrated the fact that Facebook was dragged into the matter and was ultimately responsible.

SiliconBeat (the "tech blog" of the *San Jose Mercury News),* the *Los Angeles Times, USA Today,* and other publications are all reporting that while apparently not a direct party to the negotiations between Loop and the union, Facebook has now "approved" the collective bargaining agreement, which it had to do before the contract could go into effect. In fact, Loop and Local 853 announced in their joint press release, "The contract, which workers overwhelmingly voted to ratify, went to Facebook for its agreement as Loop's paying client before implementation." Such economic realities are the type of consideration that the NLRB's General Counsel has been urging the Board to look at in deciding whether a joint-employer relationship exists.

High-tech and new media companies often rely upon third-party vendors to provide a range of non-core support services so that their own employees can focus on their primary activities. But if, as expected, the NLRB rewrites its definition and standards for determining who is a joint employer, the risks are increasing that high-tech and new media companies, like other employers, will face the prospect of having to stand alongside their vendors as employers of the vendors' personnel, including bargaining with their unions when they are represented.

3. A Growing Role for the FTC in Regulating Workforce Management

By Daniel J. Green

The FTC may be joining other federal agencies—such as the U.S. Department of Labor, the Equal Employment Opportunity Commission ("EEOC"), and the NLRB—in regulating the employment relationship, especially in the technology industry. On May 29, 2015, the FTC indicated that it would begin scrutinizing employer social media policies. Pursuant to the FTC's new guidance, an employer should ensure that its social media policy requires employees to disclose their connection to the employer prior to endorsing any of the employer's products on social media. Without such a policy, the employer may be held liable for false advertising because of the employees' failure to make an adequate disclosure.

FTC regulations[1] require a person who endorses a product to disclose any material connections with the seller of that product that affect the endorser's credibility. For example, video game reviewers must disclose that they are paid for their reviews by the games' manufacturer. The regulations also provide that the recipient of an endorsement "should advise" the endorser that "the connection should be disclosed, and it should have procedures in place to try and monitor his postings for compliance."

Under the new guidance, employees must disclose their employment relationship when endorsing their employer's product. Employers are not expected "to monitor every social media posting" by their employees. An employer's social media policies, however, should advise employees of their disclosure obligations. Further, employers "should establish a formal program to remind employees periodically of [the employers'] policy." And if an employer learns that an employee has posted a review without an adequate disclosure in violation of company policy, the employee should be instructed to remove the review or correct it to contain a disclosure.

This guidance comes in the context of increasing FTC scrutiny of the technology industry. The FTC's guidance was issued in response to changing technology and provided specific guidance to bloggers, video game reviewers, and Internet-based businesses. The FTC has also been active in seeking to regulate crowdfunding and the sharing economy. These categories of products often blur the lines among customers, suppliers, and employees. Many sharing-economy companies specialize in creating a marketplace for labor, including car rides, pet sitting, and miscellaneous household chores. The FTC is looking to promulgate regulations that place the burden on sharing-economy businesses to protect other market participants. The agency will be accepting comments on this issue until August 4, 2015. This rapidly developing area of the law will likely spawn new regulations governing the independent contractor relationship and may even result in a new category of worker, other than employees or independent contractors, governed by a different set of regulations.

---

[1] 16 C.F.R. § 255.5.

Finally, although employers are aware that non-compete and non-solicitation agreements should be carefully drafted so as not to run afoul of the antitrust laws, the FTC may begin scrutinizing the anticompetitive effect of settlement agreements resolving these cases. The agency has been aggressively scrutinizing "pay for delay" settlement agreements in which plaintiff brand-name pharmaceutical companies pay defendant generic pharmaceutical manufacturers not to enter the market (whereas, in most settlements, the defendant pays the plaintiff). Last year, we discussed how agreements among employers not to compete for employee talent can violate antitrust law. Settlement agreements in which either party receives concessions that it could not have received had it prevailed in the lawsuit may soon be subjected to similar scrutiny. For example, settlements in which both plaintiff and defendant agree not to hire or solicit each other's employees for a period of time may soon be subject to FTC investigation.

All employers, but especially those in the technology industry, should keep abreast of new legal developments, which may come from unexpected directions. An informed employer will be better positioned to adapt to, and even shape, developments without paying to litigate the test case.

4. **Avoiding Age Discrimination Complaints in an Industry Noted for a Lack of Age Diversity**
   By Lori A. Medley

Current gender and sex discrimination lawsuits filed against various Silicon Valley companies and the reported lack of gender diversity in the technology industry have recently garnered a great deal of attention. In addition, a series of age discrimination suits over the years and increased attention in the media on the industry's recruitment practices reveal that the technology industry is also vulnerable to complaints of age discrimination.

The technology industry is often described as youth-oriented and is noted for having extreme age imbalances among employees. According to a 2013 survey conducted by Payscale.com, an online salary, benefits, and compensation information company, the median ages of employees at the technology industries' top companies fall within the range of late 20s to late 30s. Given the reported lack of age diversity, this environment makes the industry vulnerable to lawsuits from individuals who are 40 or older and protected by the Age Discrimination in Employment Act of 1967 ("ADEA") and/or state and local anti-discrimination laws. Indeed, over the years, there have been several age discrimination cases brought by individuals in their 50s and 60s against the technology industry that have attracted media attention. The cases typically involve allegations of age discrimination in the workplace that the former employees alleged led to their terminations.

The technology industry has also faced criticism that its recruitment efforts imply a discriminatory preference for younger employees. Specifically, the industry has been noted for placing advertisements for positions that appear to suggest that people within a certain age range should apply for the position. The EEOC has taken notice of this

practice and, at least in instances in which the job notices specify that the position is for "new graduates" or individuals of specific graduating classes, has viewed these job notices as illegal because they deter older applicants from applying. Generally, under the ADEA, job advertisements cannot specify age preferences unless there is a bona fide occupational qualification for the age restrictions. Employers should also take note that with the EEOC's focus on addressing systemic discrimination, in which the EEOC is investigating alleged discriminatory patterns or practices or discriminatory policies that have a "broad impact on an industry, profession, company or geographic area," employers in the technology sector could be at risk for an EEOC enforcement initiative. In addition, the increased attention on the technology industry's hiring and recruiting practices could lead to a rise in age-based failure-to-hire litigations. Indeed, this past spring, a job applicant in his 60s filed an age discrimination putative class action lawsuit alleging that a technology company failed to hire him because of his age.

Given the increased focus on diversity issues facing the technology sector, technology industry employers can take the following steps to help minimize the risk of incurring an age-biased claim:

- Carefully review all advertisements or notices for job positions to ensure that they do not, either explicitly or implicitly, suggest that only individuals of a certain age range should apply. Avoid using phrases such as "new or recent graduates" or stating in the qualifications that individuals who graduated from specific class years (such as 2007 to the present) should apply. Instead, terms such as "entry-level position" and "no experience required" would be acceptable.

- Remove all questions or inquiries from employment applications that seek to elicit information about an applicant's age unless the applicant's age is a bona fide occupational qualification that is reasonably necessary to the normal operation of the business.

- Avoid asking questions or requesting information during the interview process that could establish an individual's age, such as date of birth, year of high school graduation, etc. Even if this information does not play a deciding role in whether to hire an applicant, the hiring process could be deemed tainted. The better practice is to wait until after the individual has been hired and the person's age or date of birth is needed for payroll and/or insurance purposes to collect such information.

- Make sure that company policies and procedures are up to date and address all forms of discrimination.

- Establish and promote a corporate culture that does not tolerate discrimination in any form.

5. Robotics in the Workplace: How to Keep Employees Safe and Limit Exposure to OSHA Citations

By Valerie N. Butera, with Theresa E. Thompson (Summer Associate)

Today's workplace is rapidly changing and so is its workforce. An increasing number of jobs once performed by humans are now performed by robots, and this has not escaped OSHA's attention. In fact, an OSHA test case is currently underway regarding the protection of employees when working with robots.

The first instance of a robot-related fatality in the United States occurred July 21, 1984, in a die-cast factory. Over the subsequent 15 years, OSHA and the National Institute for Occupational Safety and Health ("NIOSH") published guidance regarding robotics safety. In light of this test case and the increasingly broad range of hazards that OSHA targets, it is likely that OSHA and NIOSH will soon update guidelines for the safety of employees who work with or around robots. Despite the age of some of the existing OSHA and NIOSH recommendations regarding safe work with robots, they provide a helpful framework for employers to rely on in their efforts to keep employees safe and avoid costly OSHA citations. Most incidents of injury occur during activities such as maintenance, programming, and adjustments of robots. To avoid such incidents, employers should consider the following fundamental areas for safety improvements.

Designing Robotic Workstations

When designing robotic workstations, there are a number of factors to consider, such as how much space the robot will need to function. This will likely be more than a human being would need to conduct the same task. Employers need to be sure that adequate clearance distances are established.

One of the most important features of a robotic workstation is a safety fence, at least six feet in height, with an electrical interlocking gate. It should not be possible to access the robotic workstation when the gate is closed. This will prevent unauthorized entry into the range of the robot's moving parts. When the gate is opened, the operation of the robot should stop. Deliberate manual action should be required to restart the robot's automatic operation. In addition, employers should:

- avoid free-standing steel posts—these create "pinch points" where an unsuspecting worker can become trapped between the post and the robot's arm;

- consider limit switches and fixed stops located near an axis of rotation or translation;

- provide barriers between the robotic equipment and the object if freestanding objects in the robot's proximity cannot be avoided; and

- be aware that safety rails, chains, ropes, and floor markings, although useful as a cautionary reminder, do not provide adequate perimeter guarding.

Another important feature of a safe robotic workstation is a presence sensing device. Presence sensing devices include light curtain installations, pressure floor mats, and ultrasonic sensors on the robot's arm. When a presence is sensed by the device, the robot is triggered to either operate at a greatly reduced speed or halt motion entirely. The ideal design includes more than one presence sensing device.

Furthermore, employers should do the following:

- Contemplate all aspects of robotic controls. Controls from which the robot can be operated should never be located within the area where the robot is working and should always be guarded against accidental operation.

- Include as much remote technology as possible so that most troubleshooting can occur outside the robot's workstation. The control panel should feature single function controls, allowing an operator to control single pieces of equipment in the workstation safely, and user-prompt displays to minimize human errors.

- Make sure that there are numerous emergency stops located in easily accessible and convenient locations, as well as a portable programming control device that contains an emergency stop.

- Consider whether an emergency stop should cut off power or trigger a braking system to avoid additional hazards like the sudden dropping of a robot's arm or flinging of a work piece.

Training for Employees and Supervisors

Extensive safety training should be provided for all employees who are expected to have any possible contact with the robot system. Workers must be familiar with all working aspects of the robot, including the full range of motion, known hazards, programming information, locations of emergency stop buttons and power sources, and the importance of safety barriers. Training should also include procedures for freeing a colleague who becomes caught. It is important to emphasize that just because a robot is stopped does not mean it will remain stopped, and just because a robot is a repeating a motion does not mean it will continue to repeat only that motion.

Newly trained employees should be closely supervised until they adjust to the robot. Training requirements do not, however, only apply to newly hired, inexperienced employees. Experienced robot programmers and operators should also receive refresher training courses that allow them to stay up to date with technological advancements and remind them of the concern for safety. Supervisors should receive the same robotics training as other employees and operate under the assumption that no one is permitted to enter the robotic workstation without first reducing the speed of the robot or halting its movement.

Establishing Policies and Procedures Regarding Robotics Safety

Employers should create written safety rules for working around robotics. These rules and procedures should be strictly enforced and violations should result in disciplinary action. Policies should require employee training, detail energy control procedures, and mandate periodic inspections. It may be advisable to establish different personnel for robotics safety to avoid conflicts of interest and assure proper supervision of robotic workstations.

Unauthorized personnel should never enter the robot workstation or access the robotic controls. Operators should never be in the area where the robot is working while the robot is operational. Lockout procedures and control panel protection should be employed. Further, a buddy system should be created, mandating the presence of another worker with access to an emergency stop any time that an employee enters the robotic workstation.

Conducting a Systematic Safety Analysis

If an employer has robotics in the workplace, it is important to conduct a systematic safety analysis to assess existing hazards and how they should be addressed. Two popular strategies for such an analysis are the Job Safety Analysis and the Fault Tree Analysis. The Job Safety Analysis involves identifying hazards faced by employees in each step that they take to complete a task and developing solutions for each hazard. When conducting this type of analysis, employers should keep in mind the variability in the way that tasks may be performed.

Alternatively, a Fault Tree Analysis begins by defining the unwanted injury event and then graphically constructing the sequence of events and conditions that could lead to that event. Failure rates and human reliability values can allow probabilities of sequences to be completed. For this analysis, knowledge of the events that could lead to an injury is essential.

Whichever type of analysis an employer conducts, it is important to ensure that selected devices and procedures are appropriate for actual and anticipated tasks and hazards, considering the robot's use, programming, and maintenance operations. Employers should evaluate maintenance policies and records to determine the degree of potential hazard exposures inside robotic workstations and ensure that robots meet current industry standards.

By taking these safety measures, employers that use robotics in the workplace can significantly reduce the risk of employee injuries and demonstrate their commitment to safety in this brave new world.

* * *

For additional information about the issues discussed above, please contact the Epstein Becker Green attorney who regularly handles your legal matters or an author of this *Take 5:*

Brandon C. Ge
Washington, DC
202/861-1841
bge@ebglaw.com

Steven M. Swirsky
New York
212-351-4640
sswirsky@ebglaw.com

Daniel J. Green
New York
212-351-3752
djgreen@ebglaw.com

Lori A. Medley
New York
212-351-4926
lmedley@ebglaw.com

Valerie Butera
Washington, DC
202-861-5325
vbutera@ebglaw.com

About Epstein Becker Green

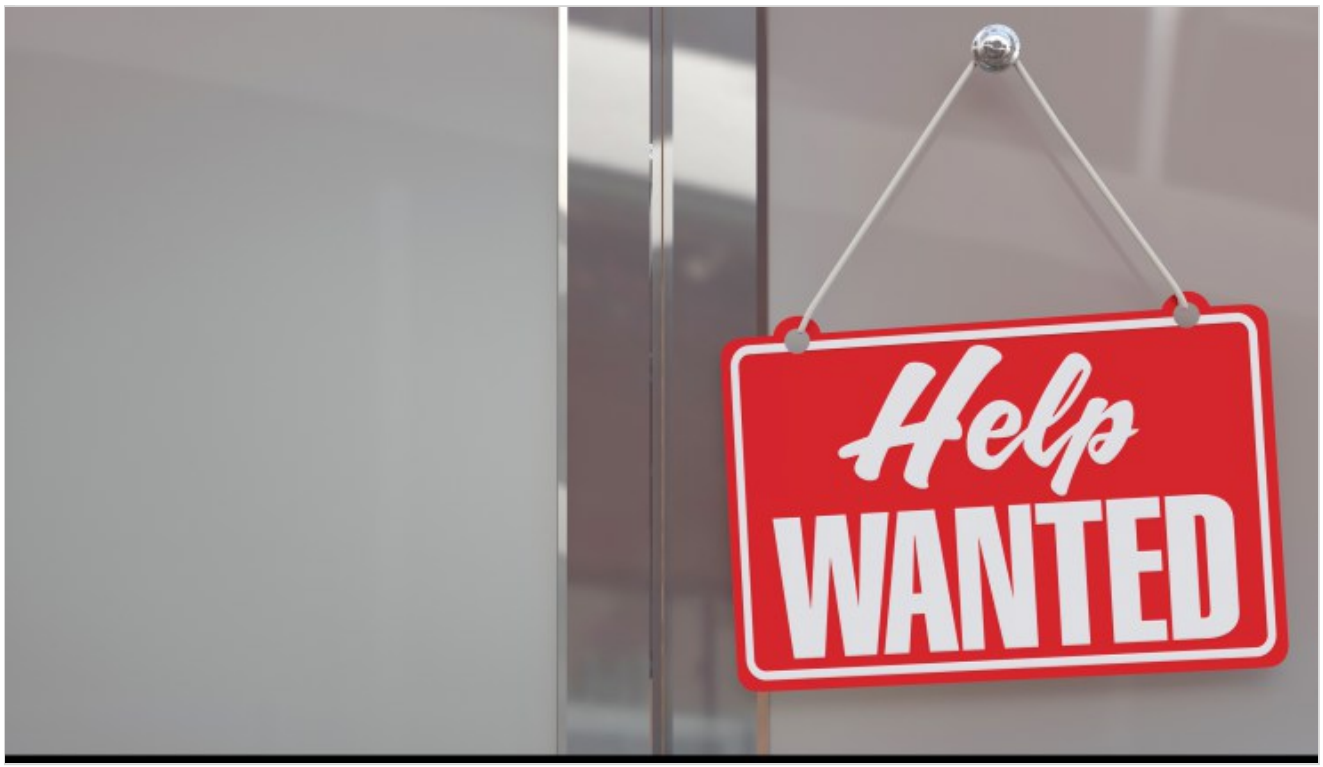
Epstein Becker & Green, P.C., is a national law firm with a primary focus on health care and life sciences; employment, labor, and workforce management; and litigation and business disputes. Founded in 1973 as an industry-focused firm, Epstein Becker Green has decades of experience serving clients in health care, financial services, retail, hospitality, and technology, among other industries, representing entities from startups to Fortune 100 companies. Operating in offices throughout the U.S. and supporting clients in the U.S. and abroad, the firm's attorneys are committed to uncompromising client service and legal excellence. For more information, visit www.ebglaw.com.

CRUNCH NETWORK

Employment Issues Your Startup Should Not Ignore

Posted Mar 13, 2015 by Ian Carleton Schaefer (@ICSTrumpet), Nancy L. Gunzenhauser

Next Story



Editor's note: *Ian Carleton Schaefer is a Member of the Firm in the Labor & Employment Department of Epstein Becker & Green's New York Office. He co-chairs the Firm's Technology, Media and Telecommunications Industry Group. Nancy L. Gunzenhauser is an Associate of the Labor & Employment Department and a member of the TMT group.*

Startups of all sizes face challenges in finding folks who want to work for them and share their vision. Hiring is tough, and welcoming these people into your organization can present "sleeper" employment law challenges and pitfalls that often go overlooked, much to the detriment of the bottom line.

Too often, startups attract talent by offering equity in the quickly growing business, either in lieu of or in addition to an employee's wages.

Unfortunately, providing stock and/or options in a company does not always adequately compensate employees under federal and state minimum-wage laws. Wage and hour lawsuits — which are up 438 percent since the year 2000, according to the Federal Judicial Center — are among the most popular and most expensive to litigate and defend.

If you're paying your people in stock in lieu of wages, you're breaking the law. Period.

Further, failure to pay overtime for employees who are not exempt from overtime (i.e. those who are ineligible for overtime by making at least $455/week *and* whose job duties fall into one of several exemptions, including executive, administrative, computer professionals) has become another minefield for startups.

There are also state law differences to remember. Overtime in Silicon Alley (for hours worked in excess of 40 for non-exempt employees) is calculated differently than overtime in Silicon Valley (which also requires the payment of daily overtime for hours worked in excess of eight in one day). So it's essential that workers are classified and paid properly to avoid substantial financial ramifications.

One of the biggest mistakes that startups make is improperly classifying their workers as independent contractors instead of employees. Whether a startup calls them "consultants," "contractors," "freelancers" or even "interns," there can be serious consequences from an employment law perspective.

The determination of who is a "contractor" and who is an "employee" is governed by both the parties' own understanding of the relationship and federal and state wage-hour laws. This guides whether someone is an employee or contractor based on multi-factor tests, and these tests vary based on jurisdiction.

Not surprisingly then, the consequences to a startup for mischaracterizing an employee as an independent contractor, including minimum wage, overtime and payroll tax violations, can be significant if not devastating.

The best way to avoid these pitfalls is to simply create an accurate job description. A good job description establishes the expectations of the job, helps the employer (and their counsel) "reality check" the position to properly classify the job, and can be used as a benchmark to evaluate applicant's "fit" and a worker's performance.

Restrictive Covenants

Intellectual property and trade secrets are among the most valuable assets many startups have. Unfortunately, many startups fail to legally protect these essential business assets through ineffective confidentiality agreements, non-competes, non-solicitations and NDAs to effectuate this end (collectively "Restrictive Covenants").

When preparing these agreements, too few founders and startups ask the critical questions: "Are my Restrictive Covenants really doing what we want them to do? "Are they truly reasonable, and will they be upheld?"

Since Restrictive Covenants are generally not self-enforcing, startups should also candidly ask themselves: "Am I willing to commit the time, money and resources to enforce these provisions in court?"

Since every state treats these types of agreements differently, it is essential that your Restrictive Covenants are properly drafted with counsel, are tailored (one size probably does not fit all) and take into account where the company may seek to enforce those agreements.

Employment policies

Most startups are not concerned with creating robust employment policies when the number of employees is small. All startups, no matter what the size, should at least have two: a sexual harassment and equal employment opportunity policy.

Under federal law (and many state and city law also counterparts), an employer can demonstrate that having a sexual harassment policy with a complaint procedure is a defense to a sexual harassment or other discrimination claim. Since several local anti-discrimination laws apply to employers with only a single employee, having an EEO policy is essential for every startup.

A sexual harassment policy is relatively simple to create and post. Establishing these policies and procedures is valuable for compliance with the laws, protecting a startup from potential litigation, staving off bad press and demonstrating to capital sources that your personnel infrastructure is sound.

Planning for the end

Just like other relationships, sometimes they just don't work out. When employees leave, it is important for startups to focus on protecting assets, including protecting against potential claims and preserving IP.

Sometimes it behooves an employer to enter into a separation agreement with a departing employee, where an employee waives his or her right to bring a lawsuit in exchange for an amount of money or other consideration. While more costly upfront, such a maneuver can save costs long-term. Startups should also focus on protecting their physical and intellectual property when employees leave the business.

Employees who use devices to access company information should either have the device returned (if company-owned) or wiped (if personally owned) to protect company data. If the departing employee has access to or managed your company's social media accounts, ensure that all passwords are either returned or changed so that the former employee cannot claim the followers or connections belong to her personally.

While it may defy common sense and a company's best intentions, it is often best to plan for the end at the beginning.

FEATURED IMAGE: MICHAEL D BROWN/SHUTTERSTOCK (IMAGE HAS BEEN MODIFIED)

The Misclassified Worker and Employee Benefit Plan Considerations

Posted on September 8th, 2015 by Michelle Capezza

If an employer is found to have misclassified an employee as an independent contractor or other contingent worker, then liability can be substantial under applicable federal and state labor, employment, tax and withholding laws including laws regarding payment of wages, overtime and unemployment compensation, workers' compensation, discrimination and rights of workers and unions. It is equally important to understand that compliance of employee benefit plans with requirements under the Employee Retirement Income Security Act of 1974 ("ERISA") and the Internal Revenue Code of 1986, (the "Code") can also be at risk. Employers must be mindful of the effects misclassification of employees can have on their employee benefit plans.

Improper exclusion of workers from participation in employee benefit plans governed by ERISA can jeopardize a plan's tax-qualified status as determined under the Code and can also provide these workers with a cause of action under ERISA. Retirement plans can lose their tax-qualified status for a variety of reasons, including as a result of "demographic failures" (where the plan does not pass coverage and nondiscrimination tests) or "operational failures" (where an employer impermissibly excludes a common law employee from plan participation believing that the worker is an independent contractor). Worker misclassification can also expose employers to penalties under the Patient Protection and Affordable Care Act for failure to properly account for the number of its employees to determine applicable large employer status as well as its failure to offer any health coverage or to offer adequate or affordable coverage to full-time employees (and their dependents). Further, the employer may be subject to penalties for violating the Code's annual informational return and statement requirements. Workers who are improperly excluded from ERISA plan participation may be able to bring a lawsuit for benefits due, to enforce rights under a plan or to clarify rights to future benefits, or raise breach of fiduciary duty claims.

Leased employees, as defined under Section 414(n) of the Code[1], also present additional challenges for plan administration and can place the qualified status of the plan at risk. Leased employees must be counted in the nondiscrimination tests of qualified retirement plans unless a safe harbor exception[2] is met. Leased employees are also counted when conducting nondiscrimination tests for other benefit plans under various provisions of the Code (such as Section 79 (group-term life insurance), Section 106 (contributions by an employer to accident and health plans), Section 125 (cafeteria plans) and Section 132 (certain fringe benefits)). Generally, where these plans do not pass applicable nondiscrimination tests, the benefits that are otherwise provided on a tax-free basis are includible in the income of the key and/or highly compensated employees benefiting under the plan. Furthermore, in the case where a leased employee converts his or her status to that of a regular employee, he or she must be credited with any periods of service previously performed for the employer for purposes of retirement plan eligibility and vesting. Prior service as a leased employee is not required to be credited for determining eligibility under a self-insured medical plan.[3]

Employers must also be careful when engaging in joint-employer relationships, especially if they have not evaluated whether they are party to such relationships or whether they are the employer of the employees. It is imperative to define in all relevant agreements and documentation which party is responsible for providing the workers with their benefits.

Plan sponsors may generally exclude from participation in employee benefit plans any leased employees or independent contractors. However, there have been situations where such individuals have challenged their non-employee classifications and their exclusion from plans. For example, in *Vizcaino v. Microsoft (120 F.3d 1006 (9th Cir. 1997))*, a class of freelancers sued Microsoft for participation in various employee benefit plans after the Internal Revenue Service determined, upon audit, that these workers were common law employees since they performed the same work as regular employees, under the same conditions and often under the same supervision. As a result of this case, many plans include a provision which provides that if a leased employee or independent contractor is reclassified as an employee by a government agency or a court, then such worker shall not become eligible to become a participant in the plan by reason of such reclassification. These types of plan provisions may be drafted to exclude participation on a retroactive basis or on both a retroactive and prospective basis, provided applicable plan coverage and nondiscrimination tests can be met. Such a provision is meant to evidence the clear intent of the plan sponsor. Furthermore, many plans also include certain *"Bruch"* language (*Firestone Tire & Rubber Co. v. Bruch*, *489*

---

[1] A leased employee is a person who provides services to a service recipient if (i) such services are provided pursuant to an agreement between the recipient and a leasing organization, (ii) such person has performed such services for the recipient on a substantially full-time basis for a period of at least one year, and (iii) such services are performed under the primary direction or control by the recipient.

[2] The safe harbor exception which allows the exclusion of leased employees from nondiscrimination testing requires that the (i) leased employees comprise not more than 20% of the service recipient's non-highly compensated workforce, (ii) leased employee is covered under the leasing organization's qualified pension plan, and (iii) the leasing organization's qualified pension plan is a money purchase pension plan that provides for immediate participation and vesting and employer contributions of at least 10% of compensation for each participant.

[3] Self-insured medical plans also undergo nondiscrimination tests under Section 105(h) of the Code and must cover at least 70% of a company's employees. If too many workers are misclassified as independent contractors, for example, a self-insured medical plan might not pass its nondiscrimination tests which could cause benefits to become taxable to highly compensated employees.

U.S. 101 (1989)) which gives the plan administrator discretionary powers to interpret the plan itself and make determinations of fact with respect to such issues as eligibility for benefits, which can only be overturned by a court if the decision is deemed arbitrary and capricious.

It is important for employers to self-audit their worker classifications and to review benefits issues as part of any analysis, such as:

- Benefit plan eligibility terms and distinctions between definition of employees, independent contractors, temporary employees and leased employees to ensure proper inclusion/exclusion of workers
- Plan nondiscrimination tests and inclusion of leased employees
- Proper crediting of service for workers who have converted to employee status
- Plan language regarding treatment of workers following reclassification and plan administrator discretion
- Consistency of provisions in all plan related documents, policies, procedures, communications and agreements regarding eligibility for benefits and excluded workers

Once an initial assessment is completed, decisions should be made as to any plan and related document revisions, or any corrective plan action, which may be required.

Lessons from the Sony Hack: The Importance of a Data Breach Response Plan

Posted on June 23rd, 2015 by Nathaniel M. Glasser and Adam Solander

In a decision emphasizing the need for employers to focus on data security, on June 15, 2015, the U.S. District Court for the Central District of California refused to dismiss a lawsuit filed by nine former employees of Sony Pictures Entertainment who allege the company's negligence caused a massive data breach. *Corona v. Sony Pictures Entm't, Inc.*, Case No. 2:14-cv-09600 (C.D. Ca. June 15, 2015).

In November 2014, Sony was the victim of a cyber-attack, which has widely been reported as perpetrated by North Korean hackers in relation for "The Interview," a Sony comedy parodying Kim Jong Un. According to the complaint in this case, the hackers stole nearly 100 terabytes of data, including sensitive personal information, such as financial, medical, and other personally identifiable information ("PII"), of at least 15,000 current and former Sony employees. The hackers then posted this information on the internet and used it to threaten individual victims and their families. The nine named plaintiffs purchased identity protection services and insurance, as well as took other measures, to protect their compromised PII.

The plaintiffs filed a class action lawsuit alleging Sony failed to implement and maintain adequate security measures to protect its employees' PII, and then improperly waited at least three weeks to notify plaintiffs that their PII had been compromised. The plaintiffs asserted claims of negligence, breach of implied contract, and statutory violations of California, Virginia, and Colorado law.

Sony moved to dismiss the complaint. First, Sony argued that plaintiffs lacked standing because they had not alleged a current injury or a threatened injury that is currently impending. The court disagreed, concluding that the allegations of increased risk of future identity theft sufficiently established certainly impending injury.

Sony then challenged the viability of each claim. While the court dismissed certain of the claims, the court allowed the plaintiffs to proceed with their claims of negligence and violations of California's Confidentiality of Medical Information Act and Unfair Competition Law. Key to the court's decision on the negligence claim were its findings that (a) the costs plaintiffs incurred

related to credit monitoring, identity theft protection, and penalties resulting from frozen credit constituted a cognizable injury, and (b) an exception to the economic loss doctrine applied because the parties had a "special relationship" whereby plaintiffs had to provide their PII to Sony in order to get paid and receive benefits.

Regarding the Confidentiality of Medical Information Act claim, the court found sufficient the allegations that Sony failed to maintain the confidentiality of the plaintiff's medical information, which Sony has admitted included HIPAA-protected health information, and failed to institute reasonable safeguards to protect that information from unauthorized use.

While it remains to be seen whether the plaintiffs will prevail on any of their theories of recovery against Sony, this matter should be a lesson to companies that have not implemented appropriate data security measures more than just the loss of proprietary information. Employers have a duty to protect the personal sensitive information that they obtain from their employees, and the failure to take preventative measures may result in legal claims, reduction in employee morale, and loss of reputation.

Employers should begin by auditing their information technology infrastructure and network for security vulnerabilities. Any such audit should be done under the supervision of counsel to maintain the privilege and confidentiality of the audit. Based on that audit, employers should take steps to mitigate the vulnerabilities found to a reasonable and appropriate level given the threats to the organization. The Sony breach, like nearly all recent breaches, had an element of social engineering. To protect against these types of attacks employers should also train their workforces on information security best practices. Finally, employers should be prepared to respond to breaches when they occur. Employers should formulate and implement a breach response plan to minimize the time from the discovery of the compromise to the reporting of the incident to affected persons.

If a data breach does occur, the company should immediately execute the data breach response plan and quickly investigate the nature and scope of the data breach. A forensic review should be conducted using an IT specialist that can trace the origins of the breach. Employees and anyone affected should be notified so that they may take appropriate steps to prevent or limit identity theft and other damages. Employers also should consider proactively notifying the police to work with the local cyber-crimes unit, as well as filing a civil suit against the perpetrator(s) to obtain injunctive relief and reduce further damage. Appropriate legal counsel can assist in pursuing these options.

Epstein Becker Green's Wage and Hour App Now Includes All 50 States and More

Posted on August 25th, 2015 by Michelle Capezza

Wage and hour issues are on the rise in every industry, and tech is no exception. (Especially see our post "How The Apple Class Certification Ruling Affects All Tech Companies.")

Our colleague **Michael Kun**, leader of our Wage and Hour group, has just announced the release of a new, expanded version of the firm's **Wage & Hour Guide for Employers app.** Available without charge for Apple, Android, and BlackBerry devices, the app is a handy, mobile reference guide to wage and hour regulations – now in all 50 states, plus federal, District of Columbia, and Puerto Rico.

Following is from the announcement:

> We have just updated the app, and the update is a significant one.
>
> While the app originally included summaries of federal wage-hour laws and those for several states and the District of Columbia, the app now includes wage-hour summaries for all 50 states, as well as D.C. and Puerto Rico.
>
> Now, more than ever, we can say that the app truly makes nationwide wage-hour information available in seconds. At a time when wage-hour litigation and agency investigations are at an all-time high, we believe the app offers an invaluable resource for employers, human resources personnel, and in-house counsel.

Key features of the updated app include:

- New summaries of wage and hour laws and regulations are included, including 53 jurisdictions (federal, all 50 states, the District of Columbia, and Puerto Rico)
- Available without charge for **iPhone**, **iPad**, **Android**, and **BlackBerry** devices
- Direct feeds of EBG's **Wage & Hour Defense Blog** and **@ebglaw on Twitter**
- Easy sharing of content via email and social media
- Rich media library of publications from EBG's **Wage and Hour practice**
- Expanded directory of EBG's Wage and Hour attorneys

If you haven't done so already, we hope you will download the free app soon. To do so, you can use these links for **iPhone**, **iPad**, **Android**, and **BlackBerry**.

Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Considering Best Data Practices For ERISA Fiduciaries

Law360, New York (May 5, 2015, 1:32 PM ET) --

Michelle Capezza

Employee benefit plan fiduciaries are charged with meeting a prudence standard when discharging their duties solely in the interest of plan participants and beneficiaries. With increasing regulation of benefit plans, these duties and associated responsibilities are mounting. With advancements in technology, online enrollment and access to account information, as well as benefit plan transaction processing, participant identifiable information and data have become increasingly more vulnerable to attack as it travels through employer and third-party systems.

Earlier this year, the attack on Anthem Inc.'s information technology system, which compromised the personal information of individuals under numerous health plans (including personally identifiable information, bank account and income data, and Social Security numbers), raised questions of privacy and security under the Health Insurance Portability and Accountability Act and Health Information Technology for Economic and Clinical Health Act, and there have been other similar attacks.

These cases remind us that in today's world, plan participant information, whether it be protected health information, personally identifiable information or retirement savings account information, is vulnerable to theft. Employee Retirement Income Security Act plan fiduciaries must not only act prudently in responding to a breach of their plan participants' PHI, but should also consider developing prudent policies and procedures with respect to the handling and transmission of all PII and participant data in the regular course.

In 2011, the Advisory Council on Employee Welfare and Pension Benefit Plans studied the importance of addressing privacy and security issues with respect to employee benefit plan administration. The council examined issues and concerns about potential breaches of the technological systems used in the employee benefit industry, the misuse of benefit data and PII and the impact on all parties, including plan sponsors, service providers, participants and beneficiaries. The council recognized several potential causes of breaches relating to benefit plan information, including hacking into retirement plan financial data, and recommended that the U.S. Department of Labor provide guidance on the obligation of plan fiduciaries to secure PII and develop educational materials. To date, the the Department of Labor has issued no such guidance.

What are the Concerns Identified by the Council?

Some of the concerns and areas of vulnerability addressed by the council include: (1) theft of personal identities and other PII, (2) theft of money from bank accounts, investment funds and retirement accounts, (3) unsecured/unencrypted data, (4) outdated and low-security passwords, (5) hacking into plan administration, service provider and broker systems, (6) email hoaxes and (7) stolen laptops or data hacked from public computers where participants logged into accounts.

The council concluded that addressing these issues requires consideration of all stakeholders who share, access, store, maintain and use PII, including, but not limited to, participants, plan sponsors, plan administrators, third-party administrators, record-keepers, investment advisors, other service providers, trustees and other fiduciaries. Issues to be considered, as set forth by the council, include privacy policies which address who may have access to PII, procedures for disseminating information concerning PII security breaches and remediation when breaches result in financial harm to plan participants and/or beneficiaries.

Developing a roadmap to remediation of financial harm may be easier said than done, however, especially given the difficulty in measuring a financial injury that may or may not occur in the future as a result of PII being stolen from an employee benefits plan or an individual participant's account. Social Security numbers, for example, may not be used to steal an individual's benefits for many years after a data breach and any subsequent lawsuit. Even if theft of Social Security numbers is directly linked to a quantifiable financial loss, plans that outsource record-keeping responsibilities to third-party administrators place fiduciaries in uncharted waters if the plan is governed by state laws that prohibit the disclosure of Social Security numbers to third parties.

Indeed, drafting an appropriate PII privacy and protection policy is quickly complicated by the sheer fact that this area of concern is evolving and questions regarding ERISA preemption and conflicts with state and federal data privacy laws are not yet definitively addressed. With federal cybersecurity legislation on the horizon, state laws on data breach notification already on the books, scrutiny over financial institutions and their compliance with laws designed to protect PII, and the increasing importance on HIPAA and HITECH compliance in the wake of health plan data breaches, merely understanding the ambit of ERISA fiduciary obligations to protect against employee benefit plan participant data breaches presents a challenge.

What Standard of Care Applies to Fiduciaries?

Under ERISA, a fiduciary shall discharge his duties with respect to a plan solely in the interest of the participants and beneficiaries, for the exclusive purpose of providing them benefits and defraying reasonable expenses of administering the plan. A fiduciary must do so in accordance with the documents and instruments governing the plan and with the care, skill, prudence and diligence under the circumstances then prevailing that a prudent man acting in a like capacity and familiar with such matters would use in the conduct of an enterprise of a like character and with like aims. A fiduciary may breach these duties with his or her action or inaction.

For instance, a 401(k) plan fiduciary that does not prudently select and monitor the investments offered under a plan or the managers of plan assets could potentially be held personally liable for breaching his or her fiduciary duties if participants and beneficiaries are financially harmed by imprudent investments. Department of Labor guidelines provide, however, that so long as the plan fiduciaries follow prudent

procedures to select and monitor plan investments, the fiduciaries are not necessarily liable for the performance of such investments. Although there is guidance plan fiduciaries can follow to properly select and monitor plan investments and service providers, as pointed out in the council's 2011 report, there is no clear guidance on the level of responsibility fiduciaries have to protect PII nor the appropriate standard of due diligence that should be used to evaluate service provider controls over the security and privacy of PII.

What Should Benefit Plan Fiduciaries Do in the Absence of Clear Rules Regarding Protection of PII?

As with other plan administration responsibilities, it is important for plan fiduciaries to establish and follow prudent practices and procedures for handling and securing PII, including when the handling and securing of such data is delegated to third parties (i.e., a "PII privacy and protection policy"). It is critical for plan fiduciaries to develop appropriate protocols in these policies, evaluate the type of data and information that will be transmitted and where it will be transmitted. Keep in mind that security measures should be tailored to a particular organization depending on their role in the benefits administration and the interface between them and the other stakeholders in the plan.

When it comes to prudent selection and monitoring of plan service providers that will handle PII, due diligence of the third-party service provider's systems, data storage and encryption security are all critical. It is equally important to prudently delegate responsibilities to company personnel that will handle PII.

Plan sponsors and other fiduciaries are well-advised to consider the following when preparing individualized PII privacy and protection policies and to require third-party service providers to demonstrate compliance.

Data

- Keep only data that is needed and use effective processes to discard unnecessary data, including backup paper and electronic copies.

- Know where PII is located in all of the organization's systems, and understand the security levels of any cloud computing and remote data storage processes that are involved in plan administration, including how data is stored or protected.

- When protected health information is at issue, follow HIPAA/HITECH guidelines.

Systems

- Keep computer systems updated, including prompt installation of software patches and stay current on electronic threats and effective responses.

- Follow National Institute of Security and Technology guidelines on computer configuration use.

- Use full disk encryption on laptops and external data storage devices that might include PII or information on how to access it.

- Maintain complete login for the network, firewalls, routers and key software applications, and limit or define usage of portable devices.

Service Provider Management

- Delegate duties responsibly and prudently monitor third parties and employees with access to plan data.

- Address privacy and security factors when vetting and selecting providers.

- Assess the service providers' certifications in privacy and security and request information regarding past data breaches.

- Request information regarding service providers' processes and systems for addressing cybersecurity threats and protection of PII.

- Make sure third-party provider subcontractors are held to same standards as the service provider.

- Develop a record of diligence efforts undertaken to document the level of security of third-party service providers and that their systems and methods for handling, storing and retrieving data are compliant with state of the art security measures.

- Engage the expertise of company IT professionals and your legal counsel to review service agreements and provisions regarding data security and confidentiality, and develop parameters for indemnification in service agreements.

- Review a copy of each third-party service provider's Statement of Auditing Standards No. 70 report regarding its system controls.

Special Concerns for Employees

- Educate employees about the importance of safeguarding their data at all times and warn against email and phishing scams.

- Encourage use of passwords with a high level of security and that they are updated regularly.

- Advise participants and beneficiaries to monitor their accounts.

- Focus on security measures in place for plan distributions, loans and withdrawals. Ensure added security for participants at time of distribution.

- Prepare communications that remind participants and beneficiaries to safeguard their own benefit information, account balances, health information, passwords and PINs, and advise against placing too much personal information on social networking sites and reviewing sensitive data on public computers or kiosks.

People and Training

- Perform background checks on all individuals with access to PII.

- Ensure all personnel who have access to PII are trained in properly safeguarding it. Include training in areas such as data retention/destruction, social networking, social engineering and litigation holds.

- Designate an individual to be in charge of privacy and security of PII, educate all stakeholders regarding appropriate focus according to their roles, and implement and test contingency plans for use in event of data breach.

General Tips

- Keep records of any breach investigations and steps taken to remedy the breach.

- Review fiduciary liability insurance and consider potential interplay between cybersecurity insurance.

- Perform periodic risk assessments (Generally Accepted Privacy Principles), maintain good controls and be careful about who can override them.

- Consider updating plan documents to incorporate the PII protection and privacy policy.

- Use a process to confirm compliance with the policy and make sure the policy is clear and communicated to all appropriate parties.

In this ever changing landscape, these considerations are not definitive or finite. Development of best practices, including a PII privacy and protection policy, will require thought and insight depending on the facts and circumstances. In the absence of formal guidance, it is imperative for plan sponsors and fiduciaries to address these issues and develop best practices and procedures that are suitable to prudently administer their plans in the information/innovation age.

—By Michelle Capezza and August E. Huelle, Epstein Becker & Green PC

Michelle Capezza is a member of the firm and August Huelle is an associate in Epstein Becker & Green's New York office.