July 2017

Five Workforce Management Challenges in Unprecedented Times

Employers across all industries are deep in the midst of exciting but unchartered and fluid times. Rapid and unforeseen technological advancements are largely responsible for this dynamic. And while there is a natural tendency to embrace their novelty and potential, the reality is that these advancements are often outpacing our regulatory environment, our bedrock legal constructs, and, in some cases, challenging the traditional notions of work itself.

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.

For employers, this presents numerous challenges and opportunities—from the proper design of the portfolio of the modern workforce, to protecting confidential information in an increasingly vulnerable digital world, to managing resources across less and less predictable borders, and to harnessing (while tempering the power of) intelligence exhibited by machines.

The time is now (if not yesterday!) to develop a long-term strategy to help navigate these current issues and anticipate the challenges and opportunities of the future.

What follows in this edition of Epstein Becker Green's *Take 5* are just some of the most salient of the workplace issues of today and tomorrow:

1. **Embracing the Gig Economy: You're Already a Player in It (Yes, You!)**
2. **AI in the Workplace: The Time to Develop a Workplace Strategy Is Now**
3. **Best Practices to Manage the Risk of Data Breach Caused by Your Employees and Other Insiders**
4. **News Media Companies Entering the Non-Compete Game**
5. **Employers Dodge Bullet in Recent U.S. Supreme Court Travel Ban Order**

1. **Embracing the Gig Economy: You're Already a Player in It (Yes, You!)**

By Ian Carleton Schaefer and Lori A. Medley

The term "gig economy" has gotten a substantial amount of play and attention in the media and in daily life as of late—often provoking near Pavlovian mental images of ride-sharing platforms, people on bicycles frantically running errands in an urban environment, or other device-based apps and services that five years ago we couldn't envision—and which now we cannot fathom a world being without. But that common depiction and definition of the "gig economy" is, in fact, far too narrow.

Because here's the thing: whether you want to or not or whether you realize it or not, the stark reality is that all companies—old and new, large and small, public and private—historically, currently, or imminently are real players in the gig economy, or what some refer to as the "contingent workforce game."

Put simply, the "contingent workforce game" or "gig economy" refers to the labor economic model of short-term work relationships or alternative, non-traditional work relationships in which workers (whether they be self-employed, employed through employment agencies, temps, consultants, contractors, freelancers, seasonal, or the all-encompassing "other") accept assignments of various lengths from people and firms who demand their services—as opposed to the more traditional, full-time employment relationship.

While temporary employment or non-traditional working arrangements are certainly not a new concept in the U.S. economy, the ubiquity and efficiency of these arrangements today has increased the demand for new technologies and platforms to facilitate this growing human capital model. In fact, the Bureau of Labor Statistics estimates that, in 2017, as many as 40 percent of the U.S. workforce is considered contingent. This figure is expected to grow to 50 percent by 2020.

Here are five issues that all companies should be mindful of as they embark on their own journey of embracing the gig economy:

1. **Misclassification of Employees:** Identifying whether an individual is an employee or an independent contractor continues to be the most confused and contentious issue for gig workers and employers alike. The stakes are due to the afforded rights, protections, and benefits under applicable law and employer policies provided to various workers.

   The financial implications of misclassification have been known to the tech sector since at least 1997, when *Vizcaino v. Microsoft Corp.*, 120 F.3d 1006 (9th Cir. 1997), served as a wake-up call. This decision held that freelance workers who worked for Microsoft between 1987 and 1990, and who had signed independent contractor agreements noting their ineligibility for benefits, were common law employees and eligible for benefits under Microsoft's 401(k) plan and Employee Stock Purchase Plan, pursuant to the language of those plans.

   A more recent and closely watched case is *O'Connor v. Uber Techs*, 82 F. Supp. 3d 1133 (N.D. Cal. 2015). In *O'Connor*, plaintiffs, who are individuals who worked as Uber drivers, allege that they are Uber employees and should be paid minimum wage and receive reimbursement for work expenses. Uber argues that it is a technology platform that merely partners with independent contractors to connect them with consumers who need a ride. On summary judgment, the court found that the plaintiffs had established a rebuttable presumption that they were employees, focusing on the amount of control that Uber exercised over its drivers through its interview process, unilateral determination of

rates, and ability to terminate drivers who received low customer satisfaction scores. Ultimately, the question of whether the plaintiffs are employees or independent contractors was for the jury to decide. The case has yet to go to trial, and a proposed $100 million settlement was rejected by the California District Court last year. This remains a seminal case to track that will have ripple effects on the broader gig economy for years to come.

2. **Agreements with Independent Contractors:** In light of the potential for misclassification claims, it is becoming ever more important for companies to clearly define their relationships with temporary workers at the outset and memorialize the details of the relationship in an independent contractor agreement. Employers must also be mindful of applicable state law that provides a means for clarifying the independent contractor relationship. For example, on May 15, 2017, New York City's Freelance Isn't Free Act ("FIFA") took effect. Under FIFA, among other things, parties that retain "freelance workers" to provide services under a contract between them that is worth $800 or more must reduce the contract to a written agreement. Contracts with independent contractors or staffing agencies should also contain strong indemnification language to protect a company from liability should the independent contractor or temporary worker negligently or intentionally harm its customers, as well as require the contractor to maintain and furnish proof of insurance.

3. **Joint Employment/Co-Employment:** The potential to unwittingly become a joint employer with a third-party entity that is acting as an intermediary and providing the workers (i.e., a temporary staffing company) is also ranked as a chief concern among employers. The joint-employer concept looks at whether two companies share or control the essential terms and conditions of employment for a worker. If a company is deemed to be a joint employer with another employer, that company can be found equally liable for any claims or legal issues (e.g., discrimination, wage-hour violations, etc.). Any agreement with a third-party entity should, at a minimum, contain a disclaimer on joint-employer status and clearly delineate responsibilities. Contractual strategies aside, the practical difficulties involved in balancing the requisite amount of supervision to be exercised over temporary workers with the legal standards of what constitutes a joint employer makes a finding of "no joint employment" increasingly challenging.

4. **Development of Company Culture:** While the flexibility to hire individuals on a temporary basis can certainly prove beneficial, it can become increasingly difficult to cultivate a cohesive company culture in a workplace that leverages a revolving door of temporary workers, particularly in light of misclassification and co-employment risks. It is increasingly incumbent on employers to evaluate and manage their resourcing model and to assess whether the makeup of their human capital portfolio is properly balanced for their business and cultural needs.

5. **Susceptibility to Unionization:** As the demand for portable benefits and wage parity for gig workers grows, more and more non-traditional work environments may find themselves targeted for unionization and organized labor as a means of providing protection and benefits to gig workers. As a recent example, the Huffington Post editorial workers voted to unionize in 2016 and recently voted to approve their first collective bargaining agreement with the Writers Guild of America East ("WGAE"), guaranteeing a minimum pay base for editorial workers and $16 per hour pay for comment moderators. WGAE has also approved union contracts for other digital content providers.

   The rise of the gig economy has also resulted in the birth of nonprofits created to provide benefits for, and to lobby on behalf of, independent contractors, most notably the

Freelancers Union (a strong supporter in the passage of FIFA, and one whose membership has surpassed 300,000).

In the end, whether you are a company that approaches the gig economy with open arms or with some resistance—make no mistake—this not-so-new normal is here to stay, and you are already operating in it. So embrace the reality, but do take caution along your journey.

2. AI in the Workplace: The Time to Develop a Workplace Strategy Is Now

By Michelle Capezza and Adam S. Forman

When it comes to artificial intelligence ("AI"), or intelligence exhibited by machines, most people immediately think of cinema's sentient computers such as HAL, Skynet, or Samantha. Although those machines are just Hollywood's fictional creations, the underlying notion that AI will play an integral role in every aspect of our lives is very real indeed. With the exponential rate of technological change, AI will continue to affect our lives more quickly and pervasively than ever before. One area that is already being impacted is the workplace.

From algorithms analyzing employee data, to computer and robotic laborers in retail and manufacturing, to the rise of the on-demand worker, AI has already disrupted how virtually every workplace operates. There is little doubt that the time to develop a workplace strategy is now. Some of the issues that organizations should consider as they introduce AI into the workplace include:

- **HR Technology:** Whether it is people analytics, digital interview platforms, or chat bots, AI is quickly becoming mainstream in human resource departments. Fueled by efficiencies and other benefits, these AI technologies seek to combine "big data" with human insight to glean unique information about talent for and within an organization. Employers introducing these technologies should make sure to review the vendor contracts and algorithms for employment law issues, such as whether the AI accounts for people with disabilities. Monitoring to make sure that the technologies do not have a disparate impact is also advisable.

- **Union Issues:** Employers that have represented workforces may need to bargain with their labor unions over the introduction of AI into the workplace, as well as the effects of AI on represented employees. Non-represented employers should make sure that the AI does not unlawfully interfere with its employees' right to engage in organizing activities, discuss wages, hours, and other terms and conditions of employment. Care should also be taken to make sure that data captured and stored with AI is not used for purposes prohibited by federal labor law, such as for unlawful surveillance.

- **Data Privacy & Security:** Many workplace AI solutions, by their very nature, collect and store large amounts of employee personally identifiable information ("PII"). Organizations utilizing such AI should take steps to make sure that they properly store and protect their employees' PII from unauthorized access by third parties or exposure through a data breach.

- **Employee Benefits:** As more workers and jobs are displaced and/or transitioned into new workplace models, in whole or in part, by AI, the ability of workers to obtain employer-provided benefits will be compromised. As a result, the traditional social safety net that has historically been supported by employer-provided benefits, such as retirement savings and health care coverage, is ripe for increased disruption. Policymakers are already proposing solutions to the workplace reality that employers will need fewer full-time employees. For example, on May 25, 2017, U.S. Senator Mark

Warner introduced in the Senate the Portable Benefits for Independent Workers Pilot Program Act (Representative Suzan DelBene introduced a companion bill in the House), which seeks to address the lack of an employer-provided safety net for workers who are not employed in traditional full-time positions and are not eligible for such benefits. While the bill seeks to provide grants to states, local governments, and nonprofit organizations to design and innovate existing benefit approaches, it also contemplates the future creation of a national portable benefits model that would require contributions from contingent workers as well as the entities that employ them. Employers should monitor these trends as well as navigate the design and compliance of their current benefits programs in light of such realities as (1) Affordable Care Act repeal and replace efforts; (2) increased appeal of health savings accounts; (3) policy efforts to move toward payroll IRAs for retirement savings; and (4) trends to de-risk and terminate pension plans, which can also involve pension withdrawal liability. Employers should also evaluate the types of benefits their workforce values in an AI-driven workplace so that they can continue to offer programs that attract and retain their desired talent.

- **Workplace Transition Policies:** With the inevitable disruption and displacement of certain jobs as workplace models transition to the new AI realities, employers should consider developing a workplace transition policy that may include establishing guidelines for employee reductions and retirements, severance and career-transitioning programs, skills development and tuition reimbursement programs, job-sharing, and flexible work arrangements.

The proverbial genie is out of the bottle with AI in the workplace, and there is no going back. Organizations should embrace the changes but do so thoughtfully and responsibly. Just as there no single AI solution that will work for every organization, there is no one-size strategy for introducing AI into the workplace. Nevertheless, prudent organizations should evaluate their workplace management goals and objectives and start developing strategies for introducing AI into the workplace. The future is now.

3. Best Practices to Manage the Risk of Data Breach Caused by Your Employees and Other Insiders

By Brian G. Cesaratto and Robert J. Hudock

The *bad news* is that most data breaches are caused by employees and other insiders (e.g., vendors), whether intentionally or inadvertently. For example, IBM Security found that insiders were responsible for 68 percent of all network attacks targeting health care data in 2016. Hackers regularly use email and social media to conduct social engineering attacks targeting unknowing employees. Not surprisingly, the highly publicized cyber threats are increasingly concerning corporate counsel. Recently, 74 percent of corporate counsel named data breaches as their top data-related legal risk. Another survey reports that 31 percent of general counsels identify cyber security as their top concern.

The *good news* is that many insider data breaches are preventable through a formalized, well-documented, and consistently applied insider threat program compliant with applicable law, including the screening, monitoring, and regular training of employees. Indeed, a comprehensive insider threat program is now a requirement for federal contractors pursuant to Executive Order 13587, which was issued in 2011 in response to the massive data leaks by Chelsea Manning. All employers should proactively address insider threats because a failure to institute best practices to prevent insider data breaches may result in significant financial loss, negative publicity, and expensive legal action should a breach occur.

Because insider threats can be divided into malicious and unintentional threat actors, the employer's program must address both:

- A *malicious* insider is a current or former employee or a business partner who has or had authorized access to the organization's network and intentionally exceeds or misuses that access in a manner that negatively affects the confidentiality, integrity, or availability of its information or information systems.
- An *unintentional* insider is someone who, through his or her action/inaction without malicious intent, causes harm or substantially increases the probability of future harm to the confidentiality, integrity, or availability of the information or information systems.

The employer's first step is to conduct a vulnerability assessment to evaluate risks according to job position and to the most sensitive data. For example, employers routinely maintain sensitive PII on its workers (e.g., benefits information, medical leave requests, health insurance and tax information, Social Security numbers, and addresses). An employer should identify where PII, trade secrets, and other confidential business information are maintained on its systems, and the employees who have access to this critical data. Job positions that permit access to critical data or systems, or grant administrative or super user privileges, should be identified.

Once the vulnerability assessment is conducted, the employer's program may be tailored to prevent, detect, and mitigate the identified risks by these employees and to the key data. The program should include personnel policies, such as pre-hire and periodic background checks and credit monitoring, employee training, access control and electronic monitoring of employee system use, strong passwords, acceptable use policies, and employer controls on the Internet of Things ("IoT") in the workplace and Bring Your Own Devices To Work ("BYOD"). The risks of BYOD and the IoT (and resulting risks from wireless connectivity) should be addressed, including regulating the types of devices that can be worn or used in the workplace. The use of encryption for confidential data in transit and at rest, and training employees in the proper use of encryption technologies, is a critical component.

Risks from disgruntled employees, or employees with a financial motive to participate in a data breach, should be documented and monitored using baselines and other objective measures. A deviation from normal baseline system activity or a high-risk event (e.g., demotion) should result in an objective trigger for increased scrutiny. For example, federal contractors are required to institute personnel-related measures to screen for 13 areas of risk, including personal conduct that involves "questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty or unwillingness to comply with rules and regulations"; financial considerations, including a history of not meeting financial obligations, overextending financially, or financial problems that are linked to gambling or drug abuse; illegal drug use; criminal conduct; security violations; outside activities that pose a conflict with an individual's security responsibilities; and the misuse of technology systems.

Ongoing training is very important both in preventing breach and in defending against legal claims if a breach occurs. Training should occur regularly and address recent social engineering attacks (e.g., ransomware) so that employees know what to look out for. The importance of training is highlighted because one click by an employee on a link containing malware may quickly disseminate across the employer's entire system. Preventing an event from occurring is critical, particularly because an intrusion may go undetected for months or even years.

Lastly, the program must anticipate the likelihood that a breach will occur and outline a response plan. Forensic artifacts can always be used to determine who, what, when, where, and why something occurred after a breach. The employer's policies in place (e.g., consensual monitoring) should enable and facilitate any future forensic investigation and a quick response time.

In sum, cyber security is a shared organizational responsibility best addressed through an insider threat program.

4. News Media Companies Entering the Non-Compete Game

By Asa F. Smith

Non-compete agreements—agreements that restrict employees from leaving a job and working for a competitor—are standard in many industries but are relatively scarce in the media and journalism sectors. Outside of television companies restricting star talent and media companies restricting executives, it has rarely been common practice for journalists to be subject to non-compete restrictions. This landscape, however, may be changing.

Two online-based news companies (both founded in 2012) are now incorporating non-competes into their contracts. NowThis (a left-leaning social media news company with a large presence on Facebook and Twitter) and the Independent Journal Review (an opinion and news website founded by former Republican staffers) have both made news in the last month for inserting broad non-compete clauses into new hire contracts.

The Independent Journal Review clause bars employees from working at "any competing business … anywhere in the world" for six months after an employee's departure. "Competing businesses" are defined as any business that is involved in the practice of publishing news content. The NowThis clause is narrower in scope; it bars employees from working at a specified list of news media companies, including CNN, BuzzFeed, and Conde Nast.

Both of these companies may have trouble enforcing their non-compete provisions. In recent years, as companies invest more in their new hires, it has become common to try to use non-competes to prevent competitors from poaching employees and benefiting from that investment. There has been a corresponding rise in regulation and backlash on the part of those who believe this to be an unnecessary and even harmful tactic. For example, the state of California has banned the use of non-compete clauses in nearly all circumstances, and other states have seen judges increasingly refuse to enforce non-compete clauses. Additionally, the New York Attorney General's office has pursued media companies (e.g., Law360) for the use of non-compete clauses.

Takeaway

As this back and forth between employers and employees (frequently with the state on their side) continues to play out, it is best for employers to ensure that, if they include a non-compete clause in their standard contracts, it is narrowly tailored in scope and geography to ensure that it is most likely to be enforced. As always, it is best to be cognizant of each applicable state's law and craft employment agreements accordingly.

5. Employers Dodge Bullet in Recent U.S. Supreme Court Travel Ban Order

By Monica Bathija

On June 26, 2017, the U.S. Supreme Court decided to partially lift lower court injunctions that had prevented any part of President Trump's March 6, 2017, executive order ("March 6 EO") to take effect.

In pertinent part, the March 6 EO barred foreign nationals ("FNs") from six predominantly Muslim-majority countries—Iran, Libya, Somalia, Sudan, Syria, and Yemen (collectively, the "Six Countries")—from entering the United States for 90 days (and 120 days for refugees), unless they were exempt from the order. The March 6 EO replaced a much broader travel ban contained in the President's January 27, 2017, executive order ("January 27 EO"). Lower federal courts in New York and Massachusetts enjoined enforcement of both the March 6 EO and the January 27 EO based on a strong likelihood that these executive orders violated the Due Process and Equal Protection clauses of the U.S. Constitution, among other grounds.

The U.S. Supreme Court's Partial Travel Ban Order

The U.S. Supreme Court's partial travel ban order, which went into effect at 8:00 p.m. EDT on June 29, 2017, lifted limited portions of these lower court injunctions against enforcement of the March 6 EO. In its decision, the Supreme Court held that the following FNs are exempt from the partial travel ban: (1) FNs in the United States with a valid visa or a travel/entry document as of June 26, 2017; (2) U.S. permanent residents; (3) dual FNs traveling on passports issued by a non-designated country; (4) FNs seeking admission to the United States in immigrant or nonimmigrant visa classifications that reflect a "bona fide relationship" with organizations or immediate family members in the United States; (5) certain diplomatic and North American Free Trade Agreement ("NAFTA") visa holders; and (6) FNs already admitted to the United States as asylees and refugees. In the Supreme Court's view, FNs seeking admission in each of these classifications had relationships with American citizens or organizations that mitigated against the security concerns that the March 6 EO was designed to address.

After the Supreme Court's decision, both the Department of State ("DOS") and Department of Homeland Security ("DHS") offered some guidance in terms of how the partial travel ban will be applied to FNs from the Six Countries. Most importantly, both the DOS and DHS confirmed that the partial travel ban does not apply to most family-based and employment-based visa classification applications. This includes FNs seeking admission in F, H, J, K, L, M, O, P, Q, and R nonimmigrant visa classifications, because each of them reflects the "bona fide" relationship required to offset the President's security concerns. Possibly excluded from this automatic exemption are certain employment-based applications, such as those by self-petitioning individuals in the EB-1 extraordinary ability classification, that are not based upon standing job offers from U.S. employers. These individuals may have to demonstrate a formal, documented relationship with a U.S. entity or citizen to secure admission.

Bona Fide Relationship

The June 26, 2017, U.S. Supreme Court decision did not define the term "bona fide relationship;" however, the Court provided a number of examples, stating that the test is based on whether a close familial relationship exists between the individual-sponsor and beneficiary. In one of its examples, the Supreme Court noted that a close familial relationship exists between an FN and his or her mother-in-law. The guidelines issued by the DOS, however, did not recognize this as a sufficiently close relationship with respect to family-based immigration. The DOS guidance reflected a very narrow approach and indicated that only parents, mothers-in-

law, fathers-in-law, spouses, fiancés, children, adult sons, adult daughters, siblings, and half-siblings are considered to have the required close family relationship. Missing from the list were grandparents, grandchildren, brothers-in-law, sisters-in-law, aunts, uncles, cousins, nieces, and nephews.

On July 13, 2017, the U.S. District Court for the District of Hawaii rejected the DOS's definition of "close familial relationship" and ruled that grandparents, grandchildren, brothers-in-law, sisters-in-law, aunts, uncles, cousins, nieces, and nephews must also be included in the definition. As a result of this ruling, the DOS updated its FAQs on July 17, 2017, to reflect the District Court in Hawaii's broader definition.

On July 19, 2017, the Supreme Court weighed in on the District Court in Hawaii's decision. The Supreme Court affirmed the District Court in Hawaii's expanded interpretation of the family relationships exempt from the travel ban. As such, grandparents, grandchildren, brothers-in-law, sisters-in-law, aunts, uncles, cousins, nieces, and nephews will continue to fall within the broader definition of "close familial relationship" and, will, therefore, remain exempt from the travel ban.

Waiver Process

Any FNs not automatically exempt from the partial travel ban permitted by the U.S. Supreme Court's interpretation of the March 6 EO may still qualify for exemption so long as they can show that they each have a bona fide relationship with the United States—either with the individual or U.S. entity sponsor. Those FNs unable to show such a bona fide relationship may still be permitted to obtain a visa if they qualify for a waiver. In order to qualify for a waiver, the FN is required to prove each of the following: (1) the denial of entry will cause undue hardship, (2) his or her entry will not pose a threat to national security, and (3) his or her entry into the United States would be in the national interest. It is unclear how such waivers will be processed or even adjudicated.

Lastly, it is important to note that, even if an FN from one of the Six Countries is successful in obtaining a visa to travel to the United States, he or she must still demonstrate admissibility at the port of entry to the U.S. Customs & Border Protection ("CBP"). The CBP retains significant discretion to deny admission to FNs, even those with valid visas, if the agency feels that the FN presents a security or other threat. Time will soon tell how CBP decides to handle the entry of FNs from the Six Countries.

Takeaway

The partial travel ban allowed by the U.S. Supreme Court does not impact employers or those they sponsor. The Supreme Court issued only an interim order, so further changes could be made once the Court hears the case in October and makes its final decision. That being said, employers should identify all employees who were born in, or are citizens of, one of the Six Countries in order to be prepared to respond to any future developments.

* * *

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:*

Monica Bathija
San Francisco
415-399-6027
mbathija@ebglaw.com

Michelle Capezza
New York
212-351-4774
mcapezza@ebglaw.com

Brian G. Cesaratto
New York
212-351-4921
bcesaratto@ebglaw.com

Adam S. Forman
Detroit (Metro) / Chicago
248-351-6287 / 312-499-1468
aforman@ebglaw.com

Robert J. Hudock
Washington, DC
202-861-1893
rhudock@ebglaw.com

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

Ian Carleton Schaefer
New York
212-351-4787
ischaefer@ebglaw.com

Asa F. Smith
New York
212-351-4599
afsmith@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.

May 2017

Employee Mobility and Trade Secret Protection in California: What Works and What Doesn't

---

California has always been a challenging jurisdiction for employers in terms of limiting unfair competition by former employees and protecting trade secrets. However, employers in the state can significantly enhance their ability to protect their business interests in these areas with a little planning and strategic thinking.

In this issue of *Take 5*, we look at some proactive steps that employers can take to prevent unfair competition by departed employees and protect trade secrets from misappropriation:

For the latest news and insights concerning trade secret and non-compete issues and trends, please visit and subscribe to Epstein Becker Green's *Trade Secrets & Noncompete Blog*.

1. **Critical Importance of Realistically Identifying and Protecting Trade Secrets and Confidential Information**

2. **Developing a Plan for Employee Departures in California**

3. **California Non-Competes: Things You Can Do "Around the Edges"**

4. **What Will Not Work to Protect Trade Secrets or Enforce Non-Competes in California**

5. **View from the Courtroom: What to Expect When You Try to Get a TRO in Your Unfair Competition Case**

1. Critical Importance of Realistically Identifying and Protecting Trade Secrets and Confidential Information

By James A. Goodman and Amy B. Messigian

California employers often face an upward battle when it comes to protecting against competitive activity by former employees. In addition to expressly precluding non-compete contracts under California Business and Professions Code ("B&P") Section 16600, California imposes hurdles to pursuing claims against former employees for taking business information that is confidential but does not rise to the level of a trade secret. Moreover, the California Code of Civil Procedure further limits employers from bringing a trade secret claim under California's Uniform Trade Secrets Act ("UTSA") unless the employer can, as a threshold matter, identify the purported trade secrets with "reasonable particularity."[1] This impedes companies from using the mechanisms of discovery to learn what an employee has taken in order to validate a claim for trade secret misappropriation; allegedly misappropriated trade secrets must be known at the outset of litigation or the case will get dismissed. Therefore, it is important for companies to identify and properly monitor for potential misappropriation so that they are well positioned to bring a claim for actual or threatened misappropriation when the circumstances arise.

In order to safeguard their trade secrets, companies doing business in California need to be on the offensive to ensure that they are properly protected at both the beginning and end of the employment relationship. At the beginning of an employment relationship, employers may set the groundwork for protecting their trade secrets by entering into confidentiality and nondisclosure agreements with their employees. These agreements will help establish one element of a claim under the UTSA,[2] which is that the employer took reasonable steps to identify its trade secrets and maintain their confidentiality.[3]

While many employers take proper measures at the onset of the employment relationship by entering into trade secret and confidentiality agreements, employers also need to make sure that they are taking similar precautions at the end of the employment relationship to prevent trade secret misappropriation. At a minimum, an employer should monitor and analyze an exiting employee's use of electronic systems, such as his or her work computer, email, and any mobile drives or devices. An exit interview should also be conducted (see the second article of this *Take 5* for a detailed discussion of exit interviews).

In addition to proper monitoring at the end of the employment relationship, employers may also be able to spot instances of misappropriation by staying alert to warning signs—such as an employee working off-hours without authorization, taking home or

---

[1] Code of Civil Procedure § 2019.210.
[2] Civil Code § 3426, *et seq.*
[3] *See Thompson v. Impaxx, Inc*., 113 Cal. App. 4th 1425 (2003).

making unnecessary copies of proprietary or other confidential material, and conducting searches or downloading documents that appear unrelated to the employee's current projects. Tracking and keeping a record of an employee's electronic footprint may enable an employer to meet the requirements under Section 2019.210 of the California Code of Civil Procedure in the event of later trade secret litigation.

Further, even if an employer finds evidence or possible evidence of misappropriation, employers must be cautioned from proceeding with trade secret litigation where there is little evidence of damages or misappropriation. For example, in *FLIR Systems, Inc. v. Parrish,* the California Court of Appeal affirmed a $1.6 million attorney fee award for the defendants (former employees of the plaintiff), finding that the plaintiff's UTSA action was brought in bad faith.[4] Among other reasons, the court found bad faith because there was no evidence of economic harm to the plaintiff and no actual or threatened misappropriation. While there was evidence that the defendants downloaded confidential information onto a hard drive, the hard drive was later destroyed without being accessed. The plaintiff discovered the download only after it had already filed its complaint, which suggested that the real reason that the plaintiff filed the case was to chill competition by the defendants, who had started a rival business.

The *Parrish* case serves as a cautionary tale for employers that are keen to utilize trade secret protections as a means of circumventing California's restraints against competition. Because California strongly favors employee mobility, simply downloading confidential information may not be enough, particularly if an employer is not aware of that taking at the outset of litigation. In addition to monitoring for employee misappropriations, employers are well advised to assess potential economic harm prior to filing litigation. If the court views the litigation as an effort to restrain employees from competing—as opposed to curing an actual or threatened misappropriation—an employer may find itself not only losing the litigation but also paying attorneys' fees to its former employees under UTSA.

2. Developing a Plan for Employee Departures in California

By Peter A. Steinmeyer

As discussed elsewhere in this *Take 5*, although California employers generally cannot restrict an employee's ability to work elsewhere, California employers can protect their trade secrets and confidential information. One pillar of a successful plan to do so is having an employee departure protocol.

The foundation of a solid employee departure protocol is the exit interview. Employers should know *who* will conduct it, *when* it will be held, and *what* will be covered.

There should be a written checklist for the exit interview, and it should cover threshold topics, such as reminding the departing employee of his or her continuing confidentiality

[4] 174 Cal. App. 4th 1270 (2009).

obligations, the return of company property and information stored on-site (e.g., access cards, laptops, and iPhones), and arrangements for the return and/or destruction of company property stored off-site.

The discussion of possible company property stored off-site should cover specific locations that a departing employee might not think of unless specifically asked, including thumb drives, personally owned computers, and personal email or cloud storage accounts. Many a lawsuit has been filed over forgotten thumb drives in employee backpacks.

The departing employee should also be asked to sign a certification that he or she has or will return all of the employer's property by a date certain, and someone needs to follow up to make sure this is done. The signing of such a certification reiterates the importance of the employee's confidentiality obligation. Additionally, should that certification later prove false (i.e., if it is later determined that the employee, in fact, misappropriated trade secrets), the false certification will be a critical piece of evidence in showing the reasonableness of the employer's efforts to protect itself—and maliciousness by the former employee.

If an employee is departing under suspicious circumstances, or if there is other reason to suspect possible misappropriation of trade secrets, records of the employee's computer activity in the days and weeks leading up to his or her termination should be preserved (e.g., by saving the employee's e-mails and making a forensic image of the employee's hard drive, rather than simply wiping it and reissuing it). Litigation over trade secret misappropriation frequently turns on evidence of unusual computer activity shortly before a departure. The employer should have a plan for accomplishing this, whether it be an internal resource, such as its information technology department, or an outside forensic computer firm.

Finally, depending on the facts of a particular situation, a formal "cease and desist" letter to a departed employee and/or a less threatening "reminder" letter can be a valuable tool. Such letters can come from the human resources or legal department, and not only serve as useful written reminders to the departed employee, but may also resolve a dispute without proceeding to litigation. Depending on the situation, an employer may also decide to send a copy of the "cease and desist" or reminder letter to the employee's new employer.

In conclusion, different employers have different needs with respect to the protection of their trade secrets and confidential information, and reasonable precautions for one employer might be completely unreasonable for another. However, regardless of the size or nature of the business, every employer should develop and maintain an employee departure protocol.

3. California Non-Competes: Things You Can Do "Around the Edges"

By James A. Goodman and Amy B. Messigian

There are not many things an employer can do to prevent unfettered competition by a former employee. B&P Section 16600 states that "every contract by which anyone is restrained from engaging in a lawful profession, trade, or business of any kind is to that extent void." The statute provides three exceptions, none of which apply to the typical employer/employee relationship: (1) a person who sells the goodwill of a business or sells substantially all of its operating assets may lawfully agree to refrain from carrying on a similar business;[5] (2) a partner may, upon the anticipation of the partnership dissolution or disassociation from the partnership, lawfully agree not to carry on a similar business;[6] and (3) any member of a limited liability company may lawfully agree not to carry on a similar business.[7]

Those exceptions are not realistic business models for most companies. California courts will carefully scrutinize business structures that ostensibly fall within one of the exceptions to determine whether structures are shams created to circumvent B&P Section 16600.[8]

Outside of the three limited exceptions, one option to prevent an employee from leaving to work for a competitor is to enter into a term agreement for employment with the employee, though such an agreement may not be desirable. Employment in California is generally "at will," which means that employment may be terminated by an employer for any lawful reason, at any time. However, an employee who has a specified term agreement is less likely to be recruited by a competitor because doing so may lead to liability against the competitor for interference with, or inducing a breach of, a contract.[9] Moreover, if the employee breaches his or her employment agreement by leaving before the term has ended, the employer would have a claim against the employee for breach of contract unless the employee can show willful or permanent breach by the employer.[10] But even with a term agreement, unless the employee has unique talents (such as a professional athlete or entertainer), the employer would still be unable to enjoin the employee from working for a competitor.[11] Although the contract for a specified term provides more security for the employer against an employee leaving and competing, it also means that the employee may be terminated only if the employee

---

[5] Bus. & Prof. Code § 16601.
[6] *Id.* at § 16602.
[7] *Id.* at § 16602.5.
[8] *Bosley Medical Group v. Abramson,* 161 Cal. App. 3d 284 (1984).
[9] *See, e.g.,* California Civil Jury Instructions Series 2200; *Diodes, Inc. v. Franzen*, 260 Cal. App. 2d 244 (1968). Conversely, under California law, competitors are generally free to solicit at-will employees unless they commit an independently wrongful act. *Reeves v. Hanlon,* 33 Cal. 4th 1140 (2004).
[10] *See* Cal. Labor Code § 2925.
[11] *Id.* at § 2855.

commits a willful breach of duty, engages in habitual neglect of duty, or is incapacitated and cannot perform.[12]

If an employer is not interested in divesting itself from the at-will nature of employment, another option to induce continued employment is to provide deferred compensation as an incentive to remain employed over a number of years. An employer may offer stock with strings attached, such that an employee who resigns may be required to forfeit his or her unvested restricted stock.[13] Another alternative for high-level employees is to provide deferred compensation in a retirement plan that is subject to the Employee Retirement Income Security Act ("ERISA") and to include noncompetition or restrictive covenant language in the plan. Because ERISA preempts state law, it may be another means of avoiding California's restrictive covenant restrictions.[14] This issue has not been tested under California law.

Covenants not to solicit employees may offer some protection against competition, but the protection *actually* provided is uncertain at best. Prior to the seminal California Supreme Court decision *Edwards v. Arthur Anderson,* employee non-solicit provisions were generally considered enforceable.[15] *Edwards* established a broad interpretation of B&P Section 16600, but the issue of employee non-solicits was not before the Court and the Court stated in a footnote that it would not address the issue.[16] No California appellate court decision has addressed employee non-solicits since 2008, but many practitioners believe that, following *Edwards*'s expansive view of Section 16600, there is a reasonably good chance that employee non-solicits will be unenforceable as well. Presently, there is appellate court authority holding that employee non-solicits are valid; thus, it is unlikely that terminating an employee for refusing to sign such a covenant (or declining to hire an employee for refusing to do so) would create the same litigation risk as terminating or refusing to hire an employee for not signing an agreement that contained an unenforceable non-competition provision. Nonetheless, employee non-solicit provisions still carry some risk and have limited upsides.

As discussed in the fourth article of this *Take 5,* while an employer may not compel the enforcement of a choice-of-law or choice-of-forum provision in an agreement with an unrepresented employee, Labor Code Section 925 expressly excludes agreements with employees who are "in fact individually represented" if the employee's lawyer is involved in negotiating the terms of the forum selection or choice-of-law clause applicable to employment disputes. This carve-out means that high-level employees, who are often represented in negotiating their employment agreements, may be validly bound to choice-of-law or forum selection provisions that open the door to restrictive covenants if they are represented in the negotiation of their employment agreements.

---

[12] *Id.* at § 2924.
[13] *Schachter v. Citigroup, Inc*., No. S161385 (Cal. Nov. 2, 2009).
[14] *Lojeck v. Thomas*, 716 F.2d 675 (9th Cir. 1983).
[15] *Loral Corp. v. Moyes,* 174 Cal. App. 3d 268 (1985).
[16] *Edwards v. Arthur Anderson*, 44 Cal. 4th 937 (2008).

In summary, there is very little that an employer can do contractually to limit competition in California; however, there are mechanisms that an employer may utilize to strengthen the longevity of its relationship with its employees. Nevertheless, an employer's focus should be on ensuring that proper measures are taken to protect trade secrets, as discussed in the first article of this *Take 5.*

4. What Will Not Work to Protect Trade Secrets or Enforce Non-Competes in California

By James A. Goodman and Amy B. Messigian

B&P Section 16600 invalidates contractual restraints on a person's ability to engage in a profession, trade, or business.[17] This statute, which has been interpreted expansively,[18] expresses a strong California public policy and contains only the three limited exceptions set forth in the third article of this *Take 5*.[19]

Employers have tried to utilize various contractual provisions and constructs to circumvent this policy without success. Out-of-state employers routinely include choice-of-law provisions in employment contracts to specify that these agreements should be interpreted under the laws of a state that is generally more amenable to restrictive covenants. Even though choice-of-forum provisions that have a reasonable relationship to one or more of the parties to the contract are presumed enforceable in California,[20] that presumption does not apply when the choice-of-law provision is used to circumvent the public policy against non-competes.[21]

Employers have had better luck in the past with choice-of-forum provisions, and federal courts in California have enforced those provisions in some instances.[22] When the choice-of-forum provision is enforced, it can make it difficult on an employee who may have to defend a non-compete lawsuit in another jurisdiction, where those courts may be less inclined to apply California law to the dispute. This "loophole" was substantially closed on January 1, 2017, with new legislation that prohibits employers from requiring, as a condition of employment, that employees who primarily reside and work in California agree to litigate claims outside of California that arise in California or otherwise deprive the employee of the substantive protections of California law.[23] While an employee may nevertheless sign such agreements, they are voidable at the employee's option unless he or she was individually represented by counsel to negotiate the venue or choice-of-law provisions. The law applies to litigation and arbitration, and to any contract entered into, modified, or extended on or after January

---

[17] Bus. & Prof. Code § 16600.
[18] Edwards, *supra* note 16.
[19] Bus. & Prof. Code §§ 16601, 16602 and 16602.5.
[20] *Smith, Valentino & Smith, Inc. v. Superior Court*, 17 Cal. 3d 491 (1976).
[21] *Application Group, Inc. v. Hunter Group, Inc.*, 61 Cal. App. 4th 881 (1998).
[22] *See, e.g., Hartstein v. Rembrandt IP Solutions, LLC*, No. 12-2270, 2012 U.S. Dist. LEXIS 105984 (N.D. Cal. July 30, 2012), and *Hegwer v. American Hearing Aid Associates*, No. C 11-04942, 2012 U.S. Dist. LEXIS 24313 (N. D. Cal. Feb. 24, 2012).
[23] Cal. Labor Code § 925.

1, 2017. With respect to agreements after such date, employers will be unable to rely on choice-of-law provisions unless the employee is represented by counsel.

In addition, "narrow restraints" in contracts will not be enforced. In 2008, the California Supreme Court rejected the narrow restraint exception[24] and held that a covenant not to solicit customers was unenforceable.[25] A covenant that prohibits hiring employees[26] or penalizes an employee for competing will likewise not be enforced.[27] As discussed in the third article of this *Take 5,* it is unclear whether contractual provisions prohibiting solicitation or other conduct by a former employee will be enforced.

The creation of sham agreements that require an employee to purchase stock or other bogus constructs that attempt to come within the scope of one of the exceptions to B&P Section 16600 by suggesting that there has been a "sale of a business" will not be enforced.[28] California courts will examine the realities of the agreement to determine if the agreement complies with the statute's intent.

Employers should think twice before including the unenforceable provisions in employment contracts merely for their deterrent effect. Such a practice is risky. If an employer terminates an employee who refuses to sign an agreement that contains an unenforceable non-compete provision, such action would constitute a wrongful termination in violation of public policy and would entitle the employee to recover tort damages, including punitive damages, as well as economic damages.[29] We are not aware of any case that expressly holds that the refusal to hire an employee who refuses to sign an agreement that contains an unlawful non-compete as a condition of employment would likewise constitute tortious conduct under California law, yet strong arguments can be made that it would. Moreover, a clause that is void under Section 16600 may also violate the provisions of the California Unfair Practices Act,[30] which could subject an employer to liability for committing an unfair business practice.[31]

Given the strong protections against non-competes in California, it is too risky to require employees to sign employment agreements that contain these provisions. All employment agreements entered into with employees who live or work in California should be carefully reviewed to ensure compliance.

---

[24] Edwards, *supra* note 16.
[25] *Id.*
[26] *VL Systems, Inc. v. Unisen, Inc.*, 152 Cal. App. 4th 708 (2007).
[27] *Muggill v. Reuben H. Donnelley Corp.,* 62 Cal. 2d 239 (1965).
[28] *Bosley Medical Group v. Abramson,* 161 Cal. App. 3d 284 (1984).
[29] *D'Sa v. Playhut, Inc.*, 85 Cal. App. 4th 927 (2000).
[30] Bus. & Prof. Code § 17200, *et seq.*
[31] *Application Group, Inc. v. Hunter Group, Inc.*, 61 Cal. App. 4th 881 (1998).

5. View from the Courtroom: What to Expect When You Try to Get a TRO in Your Unfair Competition Case

By Steven R. Blackburn

Experience shows that most unfair competition or trade secret theft issues can be resolved without the need for litigation; often, an exchange of letters between the parties' respective attorneys is sufficient to resolve the matter. However, litigation is sometimes unavoidable, and when it occurs, the employers involved are often surprised by how fast an unfair competition case can move to a practical conclusion, and how little time there might be to prepare for the crucial court hearing.

The most important event in a trade secret or unfair competition litigation is the hearing when the court grants or denies a temporary restraining order, or "TRO." A TRO is essentially an emergency injunction to prevent the wrongdoing party from taking advantage of his or her illegal activities. The process begins with the filing of a complaint that looks essentially no different than any other lawsuit. The claims are usually pleaded under theories like "conversion" (i.e., theft), fraud, breach of contract, or violations of state and federal trade secret statutes. The difference is that the parties will typically find themselves before a judge in only days, or perhaps only hours, after the lawsuit is filed for a hearing that will, for all practical purposes, resolve the case. This is the TRO hearing.

Before a TRO can be granted, the court must be satisfied that the actions of the alleged wrongdoer will cause "irreparable injury" to the party seeking the TRO—in essence, that the harm being done cannot later be remedied by an award of money damages. In the unfair competition context, a TRO is typically sought to require the immediate return of misappropriated trade secret information or to enjoin the alleged wrongdoer from soliciting the other party's customers or employees. It can be challenging to prove "irreparable injury" because most wrongs can be righted at a later time with an award of money damages. For a TRO to be issued, it truly must be a situation where "the bell cannot be un-rung."

Another requirement for a TRO is that the moving party show a high likelihood that it would prevail on the merits of its claims if the case was resolved through the ordinary litigation process, ultimately culminating in a trial. In other words, the party seeking a TRO must be prepared to demonstrate to the court that there is very clear and strong evidence of actionable bad behaviors on the part of the alleged wrongdoer.

A risk of irreparable injury and a high likelihood of eventual success on the merits are typically proven to the court by declarations filed with the complaint and TRO papers. Conclusory or vague accusations of illegal conduct will not suffice; the declarations must precisely describe what, when, and how the wrongdoer engaged in unfair competition activities. The challenge of marshalling this information in a very short period of time is further complicated by the fact that unfair competition activities almost by definition are undertaken by the guilty party in secret, and, obviously, he or she is not interested in cooperating with the victims' attorneys in putting together their case.

Very commonly, the critical evidence in an unfair competition matter comes from forensic examination of IT systems, including email, phone records, and word-processing systems. With surprising regularity, the persons who engage in these sorts of activities do not-so-smart things that leave a clear trail of their wrongdoing, often committed in the final days of their employment with their former employer.

Attempting to get a TRO in an unfair competition case can require a very large amount of work and result in the accrual of significant legal fees in only a matter of days. Before initiating the litigation process, it is critical that the employer accurately assess the viability of its case. Many employers that have thought themselves to be a victim of unfair competition have been disappointed when their case simply did not hold together well enough to justify the issuance of a TRO.

The TRO hearing is often the be-all and end-all of unfair competition litigation because, if it is granted, the unfair competitive activities are immediately stopped, any stolen trade secrets are returned, and the competitive damage to the plaintiff-employer is contained or stopped. The case is usually thereafter resolved by a settlement. Essentially, if the TRO is granted, there typically is not much else of consequence to litigate between the parties.

Conversely, if a TRO is denied, the court's ruling can effectively take the wind out of the sails of the plaintiff-employer's case. The court has essentially said, "I don't see anything wrong going on here," which means that the employee or person who has allegedly engaged in unfair competition can keep doing what he or she is doing. Here again, it is a rare unfair competition case where a TRO is denied and it makes sense for the plaintiff-employer to continue pressing on with litigation against the supposed wrongdoer. In other words, if you can't prove to the judge in the context of a TRO hearing that you have a valid claim, it's probably not going to be any easier to do so later on in the litigation. And it is a very rare situation where an unfair competition claim presents the possibility of a big award of money damages that would make continuing on with protracted litigation worthwhile.

A TRO is deemed to be an "extraordinary remedy," and an employer seeking one in an unfair competition claim should expect the judge to be cautious and conservative in deciding whether to grant one. Another factor is the often surprisingly small amount of time that the applicant gets in front of the judge to prove its case. Essentially, this is a situation where the TRO applicant is trying to push its way to the head of the line in the court's crowded docket and saying, "My case can't wait … I need a court order now." Skepticism on the part of the judge should be expected.

In California, an employer pursuing a legal claim for redress of unfair competition activities should also recognize that judges in the state superior courts are often suspicious that an unfair competition claim brought by an employer against departed employees may really be a disguised attempt to restrain legitimate competition by the former employees, which, of course, the law of the state strictly prohibits.

In short, an employer going into court to address a possible unfair competition issue is an employer that really needs a good lawyer. The law is there to stop and remedy real unfair competition, but an employer that is asking a court to intervene in what may look like just a business dispute must be realistic about the merits of its case, well prepared, and well represented.

* * *

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:*

Steven R. Blackburn
San Francisco
415-399-6040
sblackburn@ebglaw.com

James A. Goodman
Los Angeles
310-557-9519
jgoodman@ebglaw.com

Amy B. Messigian
Los Angeles
310-557-9540
amessigian@ebglaw.com

Peter A. Steinmeyer
Chicago
312-499-1417
psteinmeyer@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

Trade Secrets Litigation

PETER A. STEINMEYER, EPSTEIN, BECKER & GREEN, P.C., AND ZACHARY C. JACKSON, WITH PRACTICAL LAW LABOR & EMPLOYMENT

Search the Resource ID numbers in blue on Westlaw for more.

A Practice Note discussing trade secrets litigation for employers whose employees have misappropriated trade secrets. This Note describes pre-litigation investigations, sending cease and desist letters, and contacting law enforcement. It also addresses filing a legal action, including choice of forum and choice of law, deciding whether to include the employee's new employer and third parties, common causes of action (including the Defend Trade Secrets Act of 2016), discovery, injunctive relief, damages, and attorneys' fees. It includes best practices for preparing to counter potential defenses and counterclaims and maintaining confidentiality during litigation. This Note applies to private employers and is jurisdiction-neutral. For more information on state-specific laws, see Trade Secret Laws: State Q&A Tool.

Trade secrets are often an employer's most valuable assets. When an employee or former employee misappropriates an employer's trade secrets, the employer frequently initiates litigation with several goals in mind, including:

- Preventing further unauthorized use or disclosure of its trade secrets.
- Recovering the trade secrets.
- Obtaining damages.

This Practice Note discusses trade secrets litigation. In particular, it addresses:

- Preliminary steps to consider, such as sending a cease and desist letter and contacting law enforcement.
- Filing a legal action.
- Common causes of action.
- Discovery, including expedited discovery.
- Injunctive relief, damages, and attorneys' fees.
- Best practices for preparing to counter potential defenses and counterclaims.
- Maintaining confidentiality during trade secrets litigation.

For more information on what constitutes a trade secret and how to protect trade secrets from unauthorized use or disclosure, see Practice Note, Protection of Employers' Trade Secrets and Confidential Information (5-501-1473).

PRELIMINARY STEPS

INVESTIGATING THE SUSPECTED MISAPPROPRIATION

A prompt and thorough investigation can be critical to successful trade secrets litigation. One of the first steps in an investigation is an analysis of which information of the employer is truly secret and valuable because it is secret. Next, the employer must investigate what, if any, trade secret information the employee actually misappropriated. This investigation often consists of an in-depth forensic analysis of the employee's:

- Email.
- Desktop and laptop computers.
- Handheld electronic devices.
- Office files.
- Calendar.
- Computer and telephone logs.
- Records of office access.
- Travel and expense records.

The investigation should be performed by an experienced electronic forensic analyst who not only can perform the investigation, but can later act as electronic forensic expert in support of the employer's claims.

An investigation's revelation that the employee misappropriated trade secret information is often sufficient to obtain a court order directing the employee to cease all use and disclosure of that information and return it to the employer. This result rests on the evidence or presumption that:

- As a former employee, the defendant has no authorized or legitimate purpose for using or disclosing the employer's trade secret information.
- The employer will be competitively injured by the employee's or its new employer's use or disclosure of this information.

An employer's investigation into suspected trade secrets misappropriation also typically includes gathering information about the employee's new employer and business. For more on gathering this information, see Practice Note, Preparing for Non-Compete Litigation: Best Practices for Gathering Evidence (3-516-9469).

SENDING A CEASE AND DESIST LETTER

Depending on the circumstances, a cease and desist letter can be a valuable preliminary step to litigation or a less expensive alternative. Cease and desist letters typically:

- Remind former employees of their contractual and other obligations to the employer.
- Advise them to cease and desist from conduct that violates their obligations.
- Where appropriate, demand the return of:
  - information;
  - documents; or
  - data.

Depending on the facts of a particular situation, an employer may decide to send a copy of the cease and desist letter or a similar letter to the employee's new employer. For sample letters, see Standard Documents, Restrictive Covenant Cease and Desist Letter to Former Employee (w-002-5174) and Restrictive Covenant Cease and Desist Letter to New Employer (w-002-5171).

The employer should investigate and be able to substantiate its allegations of trade secret misappropriation before sending any cease and desist letter, as its failure to do so can expose the employer to a tortious interference claim by the employee or the employee's new employer (see Preparing for Potential Counterclaims).

CONTACTING LAW ENFORCEMENT

Where criminal conduct is suspected, an employer may decide to contact law enforcement to investigate and prosecute trade secret theft, in addition to or in lieu of sending one or more cease and desist letters. Misappropriating trade secrets is a crime under various federal laws. For example, it is illegal to:

- Misappropriate trade secrets or knowingly receive misappropriated trade secrets with the intent to benefit a foreign government or a foreign agent (18 U.S.C. § 1831).
- Transport in interstate or foreign commerce stolen property worth $5,000 or more (18 U.S.C. § 2314).
- Use the mail or a wire transmission to misappropriate trade secrets as part of a scheme to defraud (18 U.S.C. §§ 1341, 1343, and 1346).

Contacting law enforcement regarding suspected trade secrets misappropriation has three main advantages:

- The mere threat of criminal prosecution and penalties may encourage employees to explain what happened.
- Prosecutions are public, and publicity may deter other employees who are contemplating similar acts.
- If an employee has misappropriated trade secrets and left the country, law enforcement can obtain evidence abroad and possibly hold foreign conspirators accountable for their involvement.

The main drawback of contacting law enforcement is the potential for disclosure of the employer's trade secrets in connection with the prosecutorial proceedings. Law enforcement officials and judges typically try to avoid disclosing sensitive, confidential, or trade secret information unnecessarily. However, the risk exists that the employer's trade secrets may be disclosed, purposefully or inadvertently, if it helps in the prosecution of the case.

FILING A LEGAL ACTION

CHOICE OF FORUM AND CHOICE OF LAW

Unless the employee and employer have signed an agreement with an enforceable and exclusive forum selection provision, the employer decides where to initiate litigation. Depending on the facts of a particular situation, an employer may have the option of filing a complaint in federal or state court. For claims arising on or after May 11, 2016, if an employer has evidence that an employee misappropriated trade secrets, it may opt to bring a claim under the Defend Trade Secrets Act (DTSA) in federal court and join state law claims in the federal action under the court's supplemental jurisdiction. Typically, the circumstances of the case help an employer determine the more advantageous option.

Note that employers with businesses or employees in California are limited in their ability to impose forum selection clauses that require the parties to litigate outside of California or apply a law other than the law of that state. For all contracts entered into, modified, or extended on or after January 1, 2017, involving any person who primarily resides or works in California, choice of law and choice of venue contract provisions are prohibited if they apply another state's law or require adjudication in another state as a condition of employment (Cal. Lab. Code § 925). For more information, see Legal Update, California to Prohibit Choice of Law and Venue Provisions in Employment Contracts (w-003-9491).

In the absence of a choice of law provision, the court decides which state's trade secrets law should be applied if the employer and employee are located in different states. Depending on the states and the case law involved, an employer may argue that the employee violated the trade secrets law of the state or states where:

- The employer electronically stored its trade secrets.
- The employee accessed the employer's trade secrets to misappropriate them.
- The employee used the employer's trade secrets to harm the employer.

For more information on determining where to file, see Practice Notes, Preparing for Non-Compete Litigation: Where to File the

Lawsuit (3-516-9469) and Choice of Law and Choice of Forum: Key Issues (7-509-6876).

DECIDING WHETHER TO INCLUDE THE EMPLOYEE'S NEW EMPLOYER IN THE ACTION

Before initiating litigation, employers must decide which parties to name in the complaint. In certain instances, an employer may be inclined to include the employee's new employer. For example, employers should consider naming the new employer if there is evidence that:

- The former employee was acting under the new employer's direction when the employee misappropriated the former employer's trade secret information.
- The new employer has agreed to indemnify the former employee for any liability arising out of the employee's move to the new employer or breach of contract with the former employer.

For more information, see Practice Note, Preparing for Non-Compete Litigation: Deciding Whether to Include the Employee's New Employer in the Action (3-516-9469).

DECIDING WHETHER TO INCLUDE THIRD PARTIES IN THE ACTION

In addition to naming former employees and their new employers, employers should consider naming any third parties who:

- Procured or assisted in the misappropriation of their trade secrets.
- Received those trade secrets.

Naming third-party defendants in the lawsuit can help ensure the return of all copies or derivatives of the trade secrets. Employers may also be able to obtain discovery more easily than using the third-party subpoena discovery process.

COMMON CAUSES OF ACTION

MISAPPROPRIATION OF TRADE SECRETS

The most common claim against former employees who use or disclose an employers' confidential, proprietary information is a claim of trade secret misappropriation. Until the DTSA was enacted in May 2016, trade secrets had been protected primarily by state law (see Defend Trade Secrets Act). Nearly all states have enacted a version of the model Uniform Trade Secrets Act (UTSA), and the requirements for stating a claim of misappropriation under the laws of those states are often similar. Typically, to state a claim under state law, employers must allege that:

- The information at issue is the employer's trade secret.
- The employee misappropriated the trade secret.
- The employee used or intended to use the trade secret in the employee's or the new employer's business.
- The employer suffered or will suffer damages.

For more information on demonstrating trade secrets misappropriation under state law, see Trade Secret Laws: State Q&A Tool: Question 9.

INEVITABLE DISCLOSURE OF TRADE SECRETS

An employer that fails to discover evidence of an employee's actual or intended misappropriation, use, or disclosure of trade secret information should consider an inevitable disclosure claim. This claim may apply where it is impossible for the former employee to perform the new job without relying on the employee's knowledge of the former employer's trade secrets, disclosing them to the employee's new employer, or both. Employers alleging this type of claim argue that it is inevitable that the former employee will:

- Use or disclose those trade secrets in the employee's new position.
- Cause injury to the former employer as a result.

Not every state recognizes claims for inevitable disclosure of trade secrets. In the jurisdictions that recognize this cause of action, employers should emphasize in their pleadings that:

- The companies are engaged in fierce competition in a niche market.
- The former employee was a high level executive privy to strategic plans or information.
- It would be impossible for the former employee to perform the new job without using or disclosing the plans or information.
- Circumstances support or highlight the employer's concern, such as the employee being dishonest or misleading about his departure from the former employer.

In *PepsiCo, Inc. v. Redmond*, the seminal case on inevitable disclosure, Pepsi introduced evidence that:

- Quaker was one of its principal competitors.
- They were engaged in a fierce competition in the new age drink niche market.
- One of Pepsi's high-level executives had been privy to its strategic plans for the next steps in its efforts to gain market share.
- A high-level executive had resigned to work for Quaker in that same niche market.
- It would have been impossible for the former employee to perform his job at Quaker in that same niche market without bearing Pepsi's strategic plans in mind.
- Its concern was well-founded because the former executive had been dishonest about the scope of his new position at Quaker when he left Pepsi.

(54 F.3d 1262 (7th Cir. 1995).)

As a practical matter, however, courts are relatively reluctant to recognize inevitable disclosure claims because:

- The claims may effectively prevent an employee from accepting a new job even where the employee is not violating any contractual or other obligation.
- There is no evidence that the employee misappropriated anything or did anything wrong.

To convince a court to apply the inevitable disclosure doctrine, the former employer should be able to demonstrate, as in *PepsiCo*, that it is in a position where its star player has left to join the rival team right before the big game with the former employer's playbook in hand.

Although some have argued that the DTSA does not allow for inevitable disclosure claims, the DTSA is clear that it does not preempt state law, and therefore has no impact on the ability to bring inevitable disclosure claims in those jurisdictions that recognize the doctrine.

For more on inevitable disclosure, see Trade Secret Laws: State Q&A Tool: Question 17 and Practice Note, Non-Compete Agreements with Employees: Protection in the Absence of Non-Competes: Inevitable Disclosure (7-501-3409).

DEFEND TRADE SECRETS ACT

Private Cause of Action

The DTSA creates a private cause of action for civil trade secret misappropriation under federal law (18 U.S.C. § 1836(b)). The new law supplements but does not preempt or eliminate the existing patchwork of state law remedies for trade secret misappropriation (see Article, Expert Q&A on the Defend Trade Secrets Act and Its Impact on Employers: How Does the DTSA Affect Existing State Non-Compete Laws? (w-002-2128)). The DTSA applies to misappropriation that occurs on or after the law's May 11, 2016 effective date.

The DTSA uses the definition of trade secret already contained in the Economic Espionage Act (18 U.S.C. § 1836(e)). Under that definition, a trade secret is business or scientific information that:

- Derives independent economic value from not being generally known to or readily accessible by the public through proper means.
- The owner has taken reasonable measures to keep secret.

(18 U.S.C. § 1839(3).)

Under the DTSA, misappropriation occurs when a person:

- Acquires a trade secret that the person knows or has reason to know was acquired through improper means.
- Discloses or uses a trade secret of another without express or implied consent and:
  - used improper means to acquire knowledge of the trade secret; or
  - knew or had reason to know that knowledge of the trade secret was derived through improper means or under circumstances giving rise to a duty to maintain its secrecy.
- Before a material change in position of the person:
  - knows or has reason to know that the information was a trade secret; and
  - acquires knowledge of the trade secret by accident or mistake.

(18 U.S.C. § 1839(b)(5).)

Improper means includes:

- Theft.
- Bribery.
- Misrepresentation.
- Breach or inducement of a breach of duty to maintain secrecy.
- Espionage through electronic or other means.

The DTSA expressly states that improper means do not include:

- Reverse engineering.
- Independent derivation.
- Any other lawful means of acquisition.

(18 U.S.C. § 1839(b)(6).)

An owner of a trade secret that is misappropriated may bring a civil action under the DTSA if the trade secret is related to a product that is used in or intended for use in interstate or foreign commerce (18 U.S.C. § 1836(b)(1)). The DTSA claim can be combined with any applicable state law claims under statutes or common law (including for misappropriation of trade secrets, breach of a confidentiality or non-competition agreement, or unfair competition). A civil action under the DTSA may be brought in US district court (18 U.S.C. § 1836(c)). A DTSA action must be brought no later than three years after the date the misappropriation either:

- Was discovered.
- Should have been discovered with reasonable diligence.

(18 U.SC. § 1836(d).)

The remedies under the DTSA are similar to those under the UTSA (see Remedies Under the DTSA).

The DTSA has no impact on existing state law inevitable disclosure theories, except to the extent that the standard for obtaining injunctive relief may be different in federal than in state court.

For more on the DTSA, see:

- Defend Trade Secrets Act (DTSA) Issues and Remedies Checklist (w-003-6953).
- Article, Expert Q&A on the Defend Trade Secrets Act and Its Impact on Employers (w-002-2128).
- Article, The DTSA Turns One, But What Has It Done? (w-007-9652).

Whistleblower Protections

The DTSA includes protections for whistleblowers who disclose trade secrets under certain circumstances by providing criminal and civil immunity under any federal or state trade secret law for the disclosure of a trade secret that either is made:

- In confidence solely for the purpose of reporting or investigating a suspected violation of law to:
  - a federal, state, or local government official; or
  - an attorney.
- In a complaint or other document filed under seal in a lawsuit or other proceeding (see Practice Note, Filing Documents Under Seal in Federal Court (5-562-9328)).

(18 U.S.C. § 1833(b).)

Employers must give employees, contractors, and consultants notice of this potential immunity in any contract or agreement entered into or amended after the effective date of the DTSA that governs the use of a trade secret or other confidential information. An employer may comply with this requirement by cross-referencing a policy document that contains the employer's reporting policy for a suspected violation of law. (18 U.S.C. § 1833(b)(3)(A) and (B).)

For a sample notice provision, see Standard Clause, Notice of Immunity Under the Defend Trade Secrets Act (DTSA) Provision (w-003-5261).

An employer that does not provide the required notice is precluded from recovering exemplary damages or attorneys' fees under the DTSA in an action against an employee to whom notice was not provided (18 U.S.C. § 1833(b)(3)(C)) (see Remedies Under the DTSA).

ADDITIONAL CLAIMS

Employers investigating suspected trade secret misappropriation or the potential inevitable disclosure of trade secrets should consider whether alternative causes of action also apply. The employer may be able to obtain compensation for damages it has suffered by using alternative avenues such as:

- Contract law.
- Tort law.
- The Computer Fraud and Abuse Act (CFAA).

Because the burden of proof and available relief are not the same under each claim, employers should consider each claim to maximize their chances of recovery. Although beyond the scope of this Note, additional claims may be available if an employer involves law enforcement to pursue claims of, for example:

- Conspiracy.
- Criminal trade secret theft under the Economic Espionage Act of 1996.
- Mail or wire fraud.

(See Contacting Law Enforcement.)

Breach of Contract

Breach of contract claims can be based on:

- A non-compete agreement if the former employee is working for a competitor in violation of the agreement.
- A non-solicitation agreement if the former employee is soliciting customers or employees in violation of the agreement.
- A nondisclosure or confidentiality agreement if the former employee disclosed confidential or trade secret information to the employee's new employer or another party.

(See Practice Notes, Protection of Employers' Trade Secrets and Confidential Information: Breach of Contract (5-501-1473) and Preparing for Non-Compete Litigation (3-516-9469)).

Tortious Interference with Contract

An employer should consider a tortious interference with contract claim against an employee's new employer. This claim may apply if the new employer was aware that the former employee was a party to a non-compete, non-solicitation, or nondisclosure agreement, and the new employer hired the employee in a capacity where the employee would violate the agreement with the old employer. (See Practice Note, Protection of Employers' Trade Secrets and Confidential Information: Tortious Interference with Contract (5-501-1473).)

Often an employer sends a cease and desist letter to the new employer before initiating legal action against it. For a sample letter, and drafting notes about the factors employers should weigh before sending a cease and desist letter, see Standard Document, Restrictive Covenant Cease and Desist Letter to New Employer (w-002-5171).

Breach of Duty of Loyalty or Fiduciary Duty

Under the laws of most states, employees owe a duty of loyalty to their employers. Employers that discover a former employee acted contrary to their interests while still employed may also have a claim for breach of the duty. (See Practice Note, Protection of Employers' Trade Secrets and Confidential Information: Breach of Duty of Loyalty or Fiduciary Duty (5-501-1473).)

For information on state common law duties prohibiting employees from disclosing employer information, see Trade Secret Laws: State Q&A Tool: Question 16.

Defamation

Employers may consider a defamation claim if a former employee or the new employer made defamatory statements to:

- The former employer's customers in an effort to encourage them to transfer their business to the new employer.
- Former coworkers in an attempt to recruit them.

For information about defamation claims, see Practice Note, Defamation Basics (w-001-0437) and Defamation Basics State Laws Chart: Overview (3-619-6023).

Unfair Competition or Tortious Interference with Business

Employers may have a claim for tortious interference if a former employee or the new employer, or both, took an unprivileged action in an effort to interfere with the former employer's business relationships. This claim is also known as tortious interference with:

- Business relations.
- Prospective economic advantage.
- Expectancy.

Violation of the CFAA

The CFAA provides a civil cause of action against employees who access a protected computer without authorization or exceed their authorized access (18 U.S.C. § 1030). In some jurisdictions, employers may have a claim under the CFAA against a former employee who accessed the employer's computer system and obtained the employer's information for an illegitimate purpose, even if the individual was still an employee at the time of access (see, for example, *Int'l Airport Ctrs, L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2005)). In other jurisdictions, courts have held that an employee's access was not without authorization and did not exceed the employee's authorized access under similar circumstances (see, for example, *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 205 (4th Cir. 2012)). The US Supreme Court has not yet weighed in on this circuit split.

DISCOVERY

Interrogatories and written document requests in trade secret misappropriation cases typically seek information about:

- The employee's skill set and duties.
- The employee's access to confidential and trade secret information, including the nature and extent of the employee's access to confidential computer databases and files.
- Any agreements between the employer and employee, including any restrictive covenants.
- The employee's acknowledgment of and agreement to the employer's policies.

- The employee's wrongful acts of appropriation, including the information and materials misappropriated.
- Collaborative or conspiratorial conduct by the employee and other employees or third parties.
- The employee's contacts and communications with the new employer.
- The employee's contacts and communications with any corporate recruiter involved in the employee's hire by the new employer.
- The policies and practices and any relevant acts of the new employer.
- Records of the new employer's knowledge or use of the former employer's trade secrets, including existing and deleted computer files.

EXPEDITED DISCOVERY

Employers requesting injunctive relief (see Injunctive Relief) should consider requesting that the court permit discovery on an expedited schedule in advance of the hearing. Employers should:

- Narrowly tailor discovery requests to the issues that are essential to the hearing on injunctive relief.
- Emphasize the potential harm the employer is attempting to prevent.
- Demonstrate the reasonableness of the requested information by attaching the proposed discovery requests to the employer's motion for injunctive relief.

OBTAINING RELIEF FOR TRADE SECRET MISAPPROPRIATION

Depending on the facts of the case, the jurisdiction, and the claims alleged, an employer should consider drafting its complaint to include a prayer for relief seeking:

- Temporary, preliminary, or permanent injunctive relief.
- A seizure order under the DTSA (see Remedies Under the DTSA).
- Monetary damages, comprised of any combination of:
  - lost profits;
  - the wrongdoer's unjust enrichment caused by the misappropriation;
  - a reasonable royalty, where damages are difficult to calculate; and
  - exemplary damages under the DTSA or applicable state law.
- Costs.
- Attorneys' fees.
- Pre- and post-judgment interest.

INJUNCTIVE RELIEF

Typically the goal in filing a misappropriation of trade secrets lawsuit is not simply to recover damages, but first and foremost to recover the trade secrets and prevent the misappropriation from inflicting any additional (and often difficult to quantify) harm on the employer. This means that in most cases, employers request that a court issue an injunction in addition to damages.

In a trade secrets case, a temporary restraining order (TRO) may:

- Direct the return of purported trade secret information.
- Prohibit the use or disclosure of trade secret information.
- Prohibit a party from violating a restrictive covenant such as a non-compete or non-solicitation agreement.

(See Practice Note, Preparing for Non-Compete Litigation: Requesting Injunctive Relief (3-516-9469).)

Federal courts traditionally consider four factors when evaluating a motion for a preliminary injunction or TRO:

- The moving party's likelihood of success on the merits.
- The likelihood that the moving party will suffer irreparable harm absent preliminary injunctive relief.
- The balance of harms between the moving party and the non-moving party.
- The effect of the injunction on the public interest.

The federal circuits vary in how they weigh these factors. Some circuits apply a balancing test, allowing a weaker showing in one factor to be offset by a stronger showing in another. Other circuits apply the traditional factors sequentially, requiring sufficient demonstration of all four before granting preliminary injunctive relief. For more on the standards for relief in federal court, see Standard for Preliminary Injunctive Relief by Circuit Chart (8-524-0128).

MONETARY DAMAGES

In addition to injunctive relief, several types of damages are typically available for trade secret misappropriation.

Employers typically request compensatory damages that result from the misappropriation of trade secrets. Under Section 3 of the UTSA, damages can include both:

- The actual loss to the employer caused by misappropriation.
- To the extent the former employee or the new employer, or both, used misappropriated trade secrets, the unjust enrichment caused by misappropriation that is not taken into account in computing the employer's actual loss.

(Unif. Trade Secrets Act § 3.)

At times, damages in trade secret misappropriation cases depend on future events or sales and, therefore, are difficult to quantify. In those cases, the damages caused by misappropriation may be measured by the imposition of liability for a reasonable royalty for the employee's unauthorized disclosure or use of a trade secret.

If willful and malicious misappropriation exists, the court may award exemplary damages. Nearly all state laws follow the UTSA and permit exemplary damages limited to double the underlying award (for example, see 765 Ill. Comp. Stat. § 1065/4(b)).

Similar damages are available under the DTSA (see Remedies Under the DTSA).

Courts have several tools at their disposal to ensure that damages are calculated accurately under the circumstances, such as the ability to:

- Appoint a special master.
- Award pre-judgment interest.
- Order an equitable accounting.

ATTORNEYS' FEES

In addition to damages, successful employers can sometimes recover the attorneys' fees they incur in bringing a trade secret misappropriation case if the misappropriation is willful and malicious. Under Section 4 of the UTSA, attorneys' fees can also be awarded to a defendant if:

- A claim of misappropriation is made in bad faith.
- A motion to terminate an injunction is made or resisted in bad faith.

(Unif. Trade Secrets Act § 4.)

The DTSA also allows for the recovery of attorneys' fees if the employer complied with the notice of immunity requirement, if applicable (see Remedies Under the DTSA).

REMEDIES UNDER THE DTSA

The remedies under the DTSA are similar to those under the UTSA. Available remedies include:

- An injunction to preserve evidence and prevent trade secret disclosure, provided that it does not:
  - prevent a person from entering into an employment relationship, and that any conditions placed on the employment relationship are based on evidence of threatened misappropriation and not merely on the information the person knows; or
  - otherwise conflict with an applicable state law prohibiting restraints on the practice of a lawful profession, trade, or business.
- Compensatory damages measured by:
  - actual loss and unjust enrichment, to the extent not accounted for in the actual loss calculation; or
  - a reasonable royalty for the unauthorized disclosure or use of the trade secret.
- Exemplary damages up to two times the amount of the damages for willful and malicious misappropriation.
- Reasonable attorneys' fees for the prevailing party if:
  - a misappropriation claim is made in bad faith;
  - a motion to terminate an injunction is made or opposed in bad faith; or
  - a trade secret was willfully and maliciously misappropriated.

(18 U.S.C. § 1836(b)(3); see also Defend Trade Secrets Act (DTSA) Issues and Remedies Checklist (w-003-6953).)

Unlike the UTSA, the DTSA also permits the court to issue an ex parte seizure order (18 U.S.C. § 1836(b)(2)). The DTSA includes protections designed to prevent abuse of this powerful remedy and only allows an ex parte seizure order under extraordinary circumstances. A party seeking an ex parte seizure order must demonstrate as a threshold matter that an order granting injunctive relief under FRCP 65 would be futile. The courts have set a high bar for making this showing.

For more information on the civil seizure of property under the DTSA, see Articles, Expert Q&A on the Defend Trade Secrets Act and Its Impact on Employers: What Remedies Are Available to Employers? (w-002-2128) and The DTSA Turns One, But What Has It Done?: Seizure Orders (w-007-9652) and Available Relief Under FRCP 65 (w-007-9652).

PREPARING FOR POTENTIAL DEFENSES AND COUNTERCLAIMS

Although a defendant's defenses may vary by claim and circumstance, employers can make their complaint less susceptible to attack by anticipating several common defenses.

THE INFORMATION IS NOT A TRADE SECRET

Former employees' and new employers' first line of defense often is claiming that the information at issue is not a trade secret. Employers should take the following steps in anticipation of that argument.

Do Not Overreach on What Is Claimed as a Trade Secret

Typically, defendants scrutinize a complaint for categories of information that are purportedly trade secrets but are actually publicly available. For example, if an employer claims that its pricing (rather than the methodology by which it sets its pricing) is a trade secret, the employee or new employer may argue that pricing is disclosed to third-party customers and potential customers and, as a result, is not secret. Employers should only claim that information is a trade secret if they have evidence to support the claim and if that information is pertinent to the facts of the case.

Consider What Information Is Common Industry Knowledge

Defendants also frequently try to undermine the claim that information is secret by arguing that the information is commonly known in the industry. To fuel that argument, defendants look to their peers at other companies that compete with the employer to obtain testimony that the other companies' employees know this information, as well. For example, if an employer claims that its manufacturing process is a trade secret, the defendant may try to obtain testimony from the employer's competitor that it knows the details of the employer's manufacturing process. Employers should consider what information may be known by the employer's competitors when deciding what information the employer should claim is a trade secret.

Explain How You Protect Your Trade Secrets

After attacking the secrecy of the information, defendants often argue that the employer did not take appropriate steps to protect the secrecy (or purported secrecy) of the information. For example, defendants may argue that:

- The employer did not have a policy defining and protecting its confidential information.
- The employer did not train its employees on its confidentiality policy.
- The employer did not follow its confidentiality policy.

- The employer permitted employees unfettered access to files, computer systems, and information.
- Employees shared this information with clients and competitors.

Employers should describe all efforts they take to protect the secrecy of their trade secrets in their complaints. All policies, training, access restrictions, and restrictive covenants that are used to protect that information should be identified. For a sample confidentiality policy, see Standard Document, Confidential Information Policy (w-005-2678).

For information on what efforts to maintain secrecy have been deemed reasonable or sufficient for trade secret protection under state law, see Trade Secret Laws: State Q&A Tool: Question 8.

THE INFORMATION WAS NOT MISAPPROPRIATED

Defendants often argue that they did not misappropriate any information. Without surveillance footage of a former employee leaving the office with files or the hard drive from the copy machine showing mass copying of sensitive files, it can be difficult to establish otherwise. An employer's initial investigation is often the key to demonstrating the information was misappropriated. Employers, therefore, should be sure their initial investigation includes reviewing any records concerning access to the physical work environment, as well as electronically stored information.

Typically, the best evidence of a former employee's misconduct is contained in the employee's computer and email. Creating a forensic image of the hard drive from the former employee's work computer and examining that forensic image and emails for any evidence of inappropriate activities can help an employer successfully demonstrate that information was misappropriated.

For more on preserving electronically stored information, see Practice Note, Preparing for Non-Compete Litigation: Preserving Electronic Evidence (3-516-9469).

For more on the defenses available under state law, see Trade Secret Laws: State Q&A Tool: Question 11.

THE MISAPPROPRIATION OR USE OCCURRED BEFORE THE DTSA'S EFFECTIVE DATE

One of the most litigated issues under the DTSA is whether the statute applies to the alleged misappropriation. The DTSA applies only to misappropriation that occurred on or after May 11, 2016, and does not apply retroactively. Prohibited conduct under the DTSA can involve one or more of the following:

- The unlawful acquisition of a trade secret.
- The improper disclosure of a trade secret.
- The unauthorized use of a trade secret.

(18 U.S.C. § 1839(b)(5).)

The DTSA applies to "any misappropriation" that occurs on or after the effective date, even though for statute of limitations purposes any continuing misappropriation is treated as one act (*Adams Arms, LLC v. Unified Weapon Sys., Inc.*, 2016 WL 5391394, at *5-7 (M.D. Fla. Sept. 27, 2016)).

Some disputes involve trade secrets acquired before the statute's effective date, coupled with post-enactment use or disclosure. Other cases involve pre-statutory use and disclosure, with subsequent disclosures occurring after the effective date. The cases have generally concluded that the DTSA may cover pre-enactment misappropriation if the misappropriation continues post-enactment (see, for example, *Syntel Sterling Best Shores Mauritius Ltd. v. Trizetto Grp., Inc.*, 2016 WL 5338550 (S.D.N.Y. Sept. 23, 2016); *Brand Energy & Infrastructure Servs., Inc. v. Irex Contracting Grp.*, 2017 WL 1105648, at *8 (E.D. Pa. Mar. 24, 2017)).

However, some cases have rejected DTSA claims where the trade secrets were used and disclosed pre-enactment (see *Avago Techs. U.S. Inc. v. Nanoprecision Prods., Inc.*, 2017 WL 412524, at *3-4, 8 (N.D. Cal. Jan. 31, 2017) (rejecting a DTSA claim where trade secret was initially disclosed pre-enactment); see also *Dazzle Software II, LLC v. Kinney*, 2016 WL 6248906 (E.D. Mich. Aug 22, 2016) (dismissing DTSA where plaintiff failed to plead with specificity conduct post-dating the DTSA's effective date)).

Litigants faced with ambiguous coverage under the DTSA should analyze whether the benefits of proceeding in federal court outweigh the costs and delay of pleading stage motion practice challenging the court's jurisdiction. Unless litigating in a non-UTSA state, the answer generally is "no," as similar remedies are likely available under state law.

PREPARING FOR POTENTIAL COUNTERCLAIMS

When considering initiating litigation, employers should consider the possibility that their former employee and his new employer may file counterclaims. The universe of potential counterclaims is limited only by the imagination of former employees and their new employers. However, counterclaims can often include claims of:

- Unpaid wages or commissions.
- Discrimination.
- Retaliation.
- Damage caused by wrongful seizure under the DTSA (18 U.S.C. § 1836(b)(2)(G)).

Recently, there has been an increase in tortious interference claims arising from cease and desist letters. To minimize the risk of a tortious interference claim, employers should avoid sending a cease and desist letter if the allegations of trade secret misappropriation may be found to be baseless. (See Standard Document, Restrictive Covenant Cease and Desist Letter to New Employer: Drafting Note: Potential Risks of Sending a Cease and Desist Letter (w-002-5171).)

MAINTAINING CONFIDENTIALITY DURING LITIGATION

Employers that file a lawsuit concerning trade secrets should take appropriate steps to prevent their trade secrets from being publicly exposed. The UTSA and many states' trade secrets laws specifically authorize courts to take appropriate steps to protect alleged trade secrets. This may include:

- Granting a protective order in connection with discovery proceedings.
- Holding in-camera hearings.

- Sealing the records of the action.
- Ordering persons involved in the litigation not to disclose an alleged trade secret without prior court approval.

(Unif. Trade Secrets Act § 5.)

Typically employers protect their trade secrets by requesting that the court enter a protective order. In general, courts are familiar with and typically willing to enter protective orders in trade secrets cases. Because they simply provide procedural protections and do not substantively affect the facts in dispute, protective orders are commonly submitted with the agreement of all parties. Many courts, however, have local rules that govern the drafting of protective orders. Therefore, the local rules should be reviewed before requesting that the court enter a protective order.

The DTSA codifies the obligation to seal trade secrets in court proceedings, a benefit which may not be as readily available in state court (18 U.S.C. § 1835). Where the court orders the civil seizure of property under the DTSA, the court may take appropriate action to protect the:

- Seized property from disclosure (18 U.S.C. § 1836(b)(2)(B)(iii)).
- Person against whom seizure is ordered from publicity (18 U.S.C. § 1836(b)(2)(C)).
- Confidentiality of seized materials unrelated to the trade secret information that was ordered seized (18 U.S.C. § 1836(b)(2)(D)(iii)).

Cyber Threats to Employee Data and Other Confidential Information Are Front and Center in 2017

By Brian G. Cesaratto and Adam S. Forman

Now more than ever it is vitally important that employers institute personnel policies and technologies, train employees, and take other affirmative steps to protect against loss of employee personally identifiable information and other sensitive data from cyber threats. The authors of this article discuss the issue, recent litigation, and steps to take to avoid data breaches.

One need only look as far as recent headlines – where the presidential election and hacking received equal billing – to understand that technology's threats are escalating. The Democratic National Committee now joins a long list of companies in various industries that have been victims of hacking, including financial services and healthcare, among many. Risks to proprietary and confidential information, affecting millions of people, and the resulting public fallout annually escalate. The dramatic end to the 2016 election year foretells an even further increase in hacking events targeting companies and institutions of all sizes in 2017.

Companies must become even more vigilant to protect their employees' personally identifiable information ("PII") and assets. It is critically important that employers institute personnel policies and technologies, train employees and take other affirmative steps to protect against loss of employee PII and other sensitive data from cyber threats.

OF CONCERN TO GENERAL COUNSELS

Not surprisingly, these trends are increasingly concerning general counsels. A recent survey reports that 74 percent of corporate counsel named data breaches as their top data-related legal risk.[1] Another survey reports that 31 percent of general counsels identify data protection and cyber security protection as their top concern.[2] The "why" behind their legal worries is easily identified; just follow the daily news reporting of multiple high profile data breaches and the ensuing multi-million dollar settlements of class action claims. General counsels recognize that a data breach will, at a minimum, result in negative publicity and a loss of confidence in the organization. There will certainly be significant financial costs to mitigate the reputational harm and other fallout.

According to a recent IBM and Ponemon Institute study, a typical data breach costs a company just over $7 million.[3] Depending on the industry involved or the state where the breach occurred, there may be obligations to report the breach to the government or to the affected persons (including current and former employees), and respond to an ensuing governmental investigation.[4] Of course, class action lawsuits, damages claims and legal defense costs are sure to follow. A company's stock may also be negatively affected, or even targeted.[5] For example, one hedge fund has purportedly embarked on a conspicuous strategy to identify and publish alleged cyber security weaknesses while selling short the company's stock.[6]

The general counsels' concerns mount even further when considering that threats from employees can be just as serious as outside attackers, and that even an employee's careless or unknowing behavior can result in as damaging a breach as one due to malicious conduct. In particular, employees who are not aware of the dangers of social engineering attacks, such as phishing and spear-phishing, may inadvertently cause a significant data breach simply by responding to a fraudulent email. For example, the attacks on the Democratic National Committee reportedly involved successful phishing and spear phishing attacks using the organization's email systems.[7] Thus, the risks are real and growing, and the concerns well founded.

WHERE TO BEGIN?

A logical starting point for a comprehensive strategy to minimize those risks is to look at the nature of the claims asserted in the ever expanding litany of breach litigations. Most significantly, employees whose PII has been disclosed will allege that the company acted negligently by failing to take due care to protect confidential data from disclosure.[8] Numerous state laws also provide for private causes of action in the event of a data breach involving personal information, including employee PII, such as social security numbers and medical information.[9]

Affected employees are likely to claim that there was breach of an express or implied contract to protect the information arising out of the terms and conditions of employment. Failure to make timely notification to affected individuals or institutions may lead to additional statutory and common law claims.[10] Moreover, the failure to

provide timely notification of the breach (which if it had been made would presumably prompt remedial measures to avoid actual identity theft) may also increase the likelihood that employee-plaintiffs can later establish standing as courts have found standing to sue where the plaintiffs have suffered identity theft attacks.[11] Thus, breach related claims target both the inadequacy of preventative measures and the timeliness and sufficiency of the company's response should a breach occur.

LITIGATION

The litigations in Enslin v. Coca-Cola Company, Corona v. Sony Pictures and In Re U.S. Office of Personnel Management Data Security Breach Litigation are illustrative of the risks to employee PII that employers should address. The lead plaintiff in the Coca-Cola litigation was a former employee who brought a class action on behalf of 70,000 putative class members alleging statutory violations and common law claims grounded in negligence. Plaintiff claimed that 55 laptop computers containing employee PII, including social security numbers, financial and banking information, driver's license information and other sensitive material for over 70,000 current and former employees maintained by Coke's human resources department were stolen by another Coke employee.[12] The complaint pointed to the lack of encryption of the employee PII as one of the primary failures to institute adequate safeguards. The claims also included assertions that the failure to provide prompt notice of the thefts to employees was grossly negligent conduct "in the face of a preventable event."

It is interesting that in making their claims, employee-plaintiffs pointed to various standards of due care that were allegedly breached:

i. the Organization for Economic Cooperation and Development framework for security of computers and networks;
ii. the United States National Institute of Standards and Technology ("NIST") standards for securing information technology systems; and
iii. the Federal Trade Commission's guide to "Protecting Personal Information: A Guide for Business."

These standards of care were purportedly breached when employee PII was retained without business need, the PII was not protected through encryption or other controls, and there lacked sound destruction practices. Although the district court dismissed the state law negligence claims as barred under the economic loss doctrine, it recognized that there are exceptions that may in other cases permit negligence claims even where there are economic damages unaccompanied by physical injury or property damage (e.g., where the plaintiffs are able to show the existence of a special relationship to protect the information).[13]

Other courts have refused to dismiss negligence claims based on similar theories on a motion to dismiss.[14] Significantly, the district court in Enslin allowed the employees' contract claims to proceed premised on the asserted "promise of employment, with

salary, benefits and secure PHI" and to safeguard PII through "privacy policies, codes of conduct, and company security policies."[15]

In Corona, plaintiffs, all former employees of Sony, asserted claims including negligence, breach of implied contract, and violation of the California Confidentiality of Medical Information Act.[16] Plaintiffs alleged that as a result of inadequate security measures, Sony's network was hacked and that among the nearly 100 terabytes of data stolen was sensitive personal information of at least 15,000 current and former Sony employees. The information, which included employee financial, medical, and other PII, was purportedly used to threaten the individuals and their families, and was posted on the internet.

Plaintiffs claimed that they face ongoing future vulnerability to identity theft, medical theft, tax fraud, and financial theft because their PII has been, and may still be, publicly available to anyone with an internet connection, and their PII has already been traded on black market websites and used by identity thieves. Plaintiffs alleged that Sony failed to encrypt data and take other protection measures in accordance with "industry safeguards."

In denying Sony's motion to dismiss the claims of negligence and violations of the California Confidentiality of Medical Information Act, the court held that the employee-plaintiffs' allegations that they were required to provide PII to Sony in order to obtain compensation and employment benefits, and that the breach was foreseeable, established a special relationship providing an exception to the economic loss doctrine.

Similarly, the class action plaintiffs in In Re: U.S. Office of Personnel Management Data Security Breach Litigation, including employees, alleged that the OPM failed to safeguard their PII (e.g., birthdates, background check information, social security numbers, financial information, emotional health related information, private facts) asserting causes of action, inter alia, in negligence, negligent misrepresentation and concealment, invasion of privacy and breach of contract.[17]

Similar to the allegations in Corona, plaintiffs alleged that the employee-plaintiffs agreed to provide their sensitive personal information in exchange for the opportunity to be considered for employment and with assurances that the information will be protected from disclosure without their consent. The complaint alleged that material security deficiencies and lack of safeguards were noted in repeated audits posing "a significant threat to its systems," and were not corrected. Among the alleged deficiencies, were lack of multi-factor identification to gain access to sensitive data, failure to terminate remote logged in sessions when employees were working out of the office, failure to encrypt sensitive data and failure to adequately train its employees "in electronic security techniques, defenses and protocols."

In sum, these cases demonstrate that the essence of the claims – whether sounding in tort, contract or statutory violation – target purported failures to exercise due care to implement the necessary safeguards in line with published standards to protect the

employees' PII. Plaintiffs' counsels have the benefit of hindsight, which is always perfect.

WHAT SHOULD EMPLOYERS DO?

So what should employers, and in particular their legal and human resources departments, without the benefit of hindsight, do in the first instance to protect their companies against these risks? The strategy should be to take precautionary personnel and other measures in line with accepted standards for protecting employee PII (e.g., NIST standards) grounded in the lessons gleaned from the above cases. The focus should be both as to employee PII at rest and in transit. The following steps should be followed:

- As to sensitive employee PII normally maintained by personnel departments (e.g., benefits information, family and medical leave requests, medical information, tax information, social security numbers, disability related information, addresses, insurance information, direct deposit and banking information, birthdates, drivers' license information) the company should identify where the data is maintained on its electronic systems, who has access and how access is obtained. This is a comprehensive analysis of personnel software and systems, including servers, individual desktops, laptops and mobile devices, to document where this information is maintained.

- The company should determine the likelihood that a particular threat will exploit a particular vulnerability to gain unauthorized access to the employee PII and the resulting business impact. A threat analysis should assess not only the impact from a potential breach of confidentiality (e.g., identity theft), but also lack of availability (e.g., a hacker may encrypt the company's personnel/payroll information with ransomware and not release it until the demanded monies are paid).

- Steps should be taken to identify and address any gaps in protections to these threats for the stored employee PII (e.g., encryption, limiting access to Human Resources personnel, strong passwords, etc.).

- There should be personnel policies regarding the dissemination of confidential employee information using the company's electronic systems. For example, human resources should ensure that there are policies and procedures requiring sending employee tax related and other confidential information by email only if there is 100 percent confidence that the intended recipient is within the organization and has requested the information. Indeed, the IRS advises that employers consider adopting written policies that govern the electronic distribution of confidential employee Form W-2s and tax related information.[18] One simple protective measure may be requiring a phone call confirmation before hitting the send button.

- In addition to procedures verifying that the recipient of sensitive PII is actually within the organization, employers should consider technologies and policies providing for use of encryption when sending personnel related PII by email or storing it, particularly on laptops or portable media. As a general matter, employers should have in place comprehensive written policies and procedures that govern the electronic sending, receiving and storage of confidential personnel related PII.

- Employers should also consider implementing available tools to reduce risks from their own employees (such as comprehensive background checks and electronic system/email monitoring of those employees with access to employee PII) consistent with applicable laws.

- The risks from employees bringing personal devices to work ("BYOD") and the "Internet of Things" (and resulting risks from wireless connectivity) should also be addressed, including through personnel policies regulating the types of devices that can be worn or used in the workplace. The uncertainty around whether these devices are secure creates a known risk that employers should be addressing in their personnel and other electronic use policies.[19]

- Once the personnel policies and technologies are in place, training is very important both in preventing breach and in defending against claims should a breach occur. Most human resources departments are in various stages of identifying and scheduling their 2017-2018 compliance training schedule. Employers should prepare their workforce to protect employee and important organizational data from cyber threats.

Human resources departments already have in place the existing training, for example, the proper use of company technology and codes of conduct, to which specific training in cyber threats is a natural fit. Indeed, the proper use of the company's email system can include education and training on guarding against spearfishing and other social engineering attacks – one of the highest vulnerabilities. In addition, human resource's mission is to know its workforce and personnel, so it is well equipped to take complex concepts and break them down to digestible nuggets of information, disseminate the information across the workforce, track the training, and provide follow up. Human resources can help their information technology professionals identify and avoid "real world" ways that employees may utilize "work arounds" to avoid IT's well-intentioned security and policy protocols (e.g., logging in as a coworker or not using a secure Virtual Private Network ("VPN") to remotely and securely send confidential information while traveling on business or working remotely from home). Human resources is well equipped to impress upon employees that they are the best defense to protect the company and their colleagues from harm. On the other hand, failure to follow proper procedures may result in job-related disciplinary action.

Lastly, employers should plan for a breach involving employee PII. Policies and procedures should be in place for responding to and investigating a breach of each system where PII is maintained. The written plan should be in place prior to breach, and

not be a reactive measure formulated ad hoc under the stress of a breach. It should include instructions, including to human resources and employee benefits personnel, and set responsibilities for the various stages of the response.

CONCLUSION

A well thought out strategy implementing a safety net of technologies, policies and training is the best defense to mitigate the risks that are causing general counsels to lose sleep at night.

Endnotes

[1] BDO Consulting's *Inside E-Discovery & Beyond: E-Discovery Complexities Driving Change* survey (Jan. 2017).

[2] TerraLex's *The General Counsel Excellent Report 2015* survey (2015).

[3] Ponemon Institute's *2016 Cost of Data Breach Study: United States* (June 2016).

[4] *See*, *e.g.*, 45 C.F.R. § 164.400-414 (requiring HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information); N.Y. Gen. Bus. Law § 899-aa ("Any person or business which conducts business in New York State, and which owns or licenses computerized data which includes private information [unencrypted or for which the encryption key was acquired] shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York State whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization."); Mich. Comp. Law § 445.72 ("Unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state, a person or agency that owns or licenses data that are included in a database that discovers a security breach, or receives notice of a security breach… shall provide a notice of the security breach to each resident of this state…"); N.J. Stat. § 56:8-163 (requiring businesses holding personal information to provide notifications when a data breach occurs); Wash. Rev. Code § 19.255.10 (requiring notification of breach of security system containing personal information).

[5] Jim Finkle and Dan Burns, *St. Jude Stock Shorted On Heart Device Hacking Fears; Shares Drop*, Reuters, Aug. 25, 2016.

[6] St. Jude brought a defamation lawsuit against Muddy Waters Consulting LLC after it purportedly identified and published alleged wireless vulnerabilities in St. Jude's implantable cardiac rhythm devices claiming that hackers can seize control of the devices while engaged in short selling St. Jude's stock. *St. Jude Med., Inc. v. Muddy Waters Consulting, LLC*, No. 16-Civ. 030002 (DWF/JSM) (D. Minn. 2016)

[7] *See, e.g.*, FBI and NCCIC's Joint Analysis Report, *GRIZZLY STEPPE – Russian Malicious Cyber Activity*, JAR-16-20296A, December 29, 2016..

[8] *See, e.g., Enslin v. Coca-Cola Company et. al.* – Complaint – Class Action – No. 14-CV-06476-JFL (E.D. Pa. 2014); *see also In re: Target Corp. Customer Data Sec. Breach Litig. – Financial Institution Cases*, MDL No. 14-2522 (PAM/JJK) (No. 261) (D. Minn. Dec. 2, 2014) (in connection with complaint by financial institutions, court refused to dismiss negligence claims finding that assertions that Target purposely disabled security features that would have prevented the breach and failed to heed the warning signs as the attackers' attack began creating a foreseeable risk of harm plausibly pled a general negligence case).

[9] *See, e.g.,* Cal. Civil Code § 56.20(a) ("Each employer who receives medical information shall establish appropriate procedures to ensure the confidentiality and protection from unauthorized use and disclosure of that information."), § 56.36(b) ("an individual may bring an action against a person or entity who has negligently released confidential information or records concerning him or her in violation of this part . . ."). As explained by the California courts, the term "released" does not connote an affirmative act on the part of the employer. *Regents of the Univ. of California v. Superior Court*, 220 Cal. App. 4th 549, 564-65 (Cal. Ct. App. 2013), *modified*, 2013 Cal. App. LEXIS 917 (Cal. Ct. App. Nov. 13, 2013) (where an employer negligently maintains confidential medical information, thereby allowing an unauthorized third person to access it, the employer may have negligently "released" the information within the meaning of the CMIA); Mich. Comp. Law § 445.86 (providing private cause of action for release of social security numbers).

[10] *See*, e.g.*,* N.Y. Gen. Bus. Law § 899-aa (authorizing attorney general action); Mich. Comp. Law § 445.72 (authorizing attorney general action).

[11] *See In re Target Corp. Data Sec. Breach Litig. – Consumer Cases*, 66 F. Supp. 3d 1154, 1159 (D. Minn. 2014) (finding that plaintiffs had standing to sue when theft of plaintiffs' identities caused them injuries that included unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees); *Cf. Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011) (in a case where defendant provided notice of breach to 27,000 employees within 30 days of breach, the court held that plaintiffs lacked any injury in fact for standing based on claims of increased risk of identity theft where no allegation that any theft had occurred as "hypothetical future" allegations do not establish standing); *see also Clapper v. Amnesty Int'l*, 133 S. Ct. 1138, 1160 (2013) (Article III standing requires the risk of future harm to be "certainly impending."); *In re SAIC Backup Tape Data Theft Litig.*, MDL No. 2360 (D.D.C. May 9, 2014) (loss of data without evidence of misuse is insufficient to establish standing). It would indeed be a thin reed, however, for an employer to failure to adequately institute protective measures in reliance on legal defenses that may (or may not) be later available if a lawsuit results from a breach of employee PII (*e.g.*, lack of standing, economic loss doctrine). *See*, *e.g.*, *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, No. 3:16-cv-00014-GPC-BLM, 2016 U.S. Dist. LEXIS 152838, at *8 (S.D. Cal. November 3, 2016) ("[i]njury-in-fact analysis is highly case specific.").

[12] *Enslin v. Coca-Cola Company et. al.* – Complaint – Class Action – No. 14-CV-06476-JFL (alleging that the data stolen including social security numbers, drivers license records, personal addresses, and other data collected and maintained by Coke's human resources departments).

[13] *Enslin v. Coca Cola Company et. al.* – Decision, No. 14-CV-006476-JFL (E. D. Pa. Sept. 29, 2015) (dismissing negligence claim because plaintiffs asserted only the existence of standard employment contract, and did not allege any fiduciary duty or reliance on employer's expertise).

[14] *See, e.g., Leibovic v. United Shore Mort*., LLC, No. 15-12639 (E.D. Mich. Oct. 28, 2016) (refusing to dismiss common law negligence claim where plaintiff consumer alleged duty arose from defendants' acceptance of PII).

[15] *Enslin.* – Decision, No. 14-civ.-006476-JFL.

[16] *Corona v. Sony Pictures Entm't, Inc.*, Case No. 2:14-cv-09600 (C.D. Ca. June 15, 2015).

[17] *In Re U.S. Office of Personnel Management Data Security Breach Litigation*, 15-Civ.-1394 (ABJ) (D.D.C. March 14, 2016) (complaint). Defendants made a motion to dismiss which was pending as of March 1, 2017.

[18] *See* IRS February 2017 phishing alert.

[19] *See*, *e.g.*, Peterson, A., *"'Internet of Things'" compounded Friday's hack of major websites*, The Washington Post, Oct. 21, 2016.