THOMPSON HINE

Business Law Update

Spring 2019

Mergers & Acquisitions

Cybersecurity, Compliance, and Culture in M&A Transactions

By Steven G. Stransky, Mike Ragan and Tony Kuhel

Corporate data and information are key assets that businesses can and should go to great lengths to protect. This data and information can range from trade secrets and intellectual property to customer lists and personal data on employees. According to Cybersecurity Ventures, global spend on cybersecurity products and services will exceed $1 trillion over the five-year period from 2017 to 2021. Additionally, there has been a substantial increase in the regulatory enforcement of data protection laws both in the United States and abroad, which may result in significant financial penalties, litigation and reputational damage.

Consequently, cybersecurity and data privacy are an integral part of the due diligence process for mergers and acquisitions (M&A). Yet, given the evolving nature of global cyber threats and the expansion of domestic and foreign data privacy laws, organizations must strive both to comply with today's cyber threats and legal landscape, and be prepared to adapt to tomorrow's. Accordingly, to better assess the value and risk of an organization in an M&A transaction, purchasers should look beyond a target's cybersecurity measures and legal compliance program, and seek to understand its culture of security and privacy.

Cybersecurity Risk

In the M&A process, a target's lack of cybersecurity measures is an immediate red flag because of the imminent risk of cyberattacks, which can endanger a target's data and physical assets, and lay the groundwork for costly lawsuits and fines. For example, in 2016, Marriott International purchased Starwood hotels in a transaction reportedly worth more than $13 billion. However, in November 2018, Marriott had to publicly disclose that Starwood's computer networks and systems

Recent News & Related Articles

- Overview of SEC's Proposed Rule Changes for Business Development Companies
- New Ohio Law Allows Remote Online Notarization
- SEC Poised to Permit ActiveShares ETF: First Non-Transparent Actively Managed ETF
- DOJ Criminally Charges Executives for Failure to Timely Report Under CPSA
- SEC Grants No-Action Relief for Initial Coin Offering
- New Jersey Enacts Limits on Employment and Settlement Agreements
- New FCC Rule Creates TCPA Reassigned Numbers Database
- Generic Drugs: Biggest Price-Fixing Case Ever?
- Opportunity Zones: What Are They and Why Should We Care?
- SEC Issues No-Action Letter Regarding Fund Board In-Person Voting Requirements

For more details on any of the topics covered in this *Business Law Update*, please contact the authors via the links at the end of each article or David R. Valz, editor-in-chief. For information on our Corporate Transactions & Securities practice, please contact Frank D. Chaiken, practice group leader.

had been compromised by a 2014 cyberattack which exposed the personally identifiable information of up to 500 million customers to cyber criminals. Marriott's stock dropped 5.6 percent following the disclosure. It has since implemented a free credit monitoring service for impacted customers, but still faces regulatory fines, class action lawsuits and significant reputational damage.

Thankfully, cybersecurity measures are fairly easy to assess in the M&A process. Purchasers should evaluate the technical, physical and administrative measures a target has implemented – or failed to implement – against industry standards. Everything from encryption and firewalls, to physical security controls and business continuity, to personnel vetting and confidentiality requirements can provide purchasers with unique insights into a target's cybersecurity posture. As highlighted by the Starwood incident, purchasers should assess a target's cyber history. Has the target been subject to a data breach or incident in recent years? If so, how did it respond? Has the target undergone penetration testing or been subject to third-party security assessments? If so, what were the results? Fortunately, these types of questions have become routine in the M&A process.

Legal Compliance

In today's interconnected world, a business may be subject to dozens – even hundreds – of domestic and foreign data protection laws. Although complying with such laws can be challenging and expensive, noncompliance can be even more costly. For example, the European Union General Data Protection Regulation (GDPR) has spawned more than 200,000 complaints within nine months of its implementation in May 2018. In January 2019, France's data protection regulator fined Google a record €50 million for failing to comply with its GDPR obligations.

These regulatory enforcement actions are not limited to foreign jurisdictions. In February 2019, the video social networking app Musical.ly (now known as TikTok) agreed to pay $5.7 million to settle an action brought by the Federal Trade Commission (FTC), alleging that the company collected personal information from children in violation of the Children's Online Privacy Protection Act. In October 2018, the FTC gave final approval to a settlement with Uber Technologies, Inc. over allegations that the ride-sharing company deceived consumers about its privacy and data security practices. The settlement includes a 20-year requirement that Uber obtain a biennial, independent, third-party assessment certifying that it has a comprehensive privacy program.

Like cybersecurity, assessing a target's compliance with data protection laws is relatively straightforward. The purchaser needs to identify, among other issues, the types of personally identifiable information a target collects during its routine business operations, such as information from its customers, employees, website users and vendors; where the information is transmitted through and stored; and to whom it is disclosed. The purchaser should then assess whether the target has implemented (and preferably documented) all the requirements applicable in the jurisdiction(s) where data subjects reside, the business is established, and the data is stored. For example, some data protection laws require businesses to have a privacy policy and a data records schedule, to dispose of sensitive information through approved means, to adhere to certain requirements when transferring data internationally, and to execute contractual agreements with third parties with whom they share personal data. Questions probing cybersecurity compliance provide the purchaser with a greater understanding of a target's overall legal compliance, and are therefore becoming increasingly routine in the M&A process.

A Culture of Security and Privacy

Although assessing a target's current cybersecurity posture and legal compliance is a significant aspect of the due diligence process, we recommend a more holistic approach involving an assessment of a target's culture of security and privacy in order to ensure that it has the necessary tools in place to adapt to new cyber threats and data privacy

requirements. On the former, businesses face staggering cyber threats from nation-states and criminal organizations. According to a March 2019 statement by the secretary of Homeland Security, "the rate at which [cyber] threats and risks are emerging is outpacing our ability to identify, assess and address them."

Data protection laws are also evolving. The California Consumer Privacy Act (CCPA) goes into force in 2020, and sets forth comprehensive new data security requirements for certain businesses that collect personal information (which is broadly defined) on California residents. In 2018, several other U.S. states, including Colorado (HB18-1128), Nebraska (LB757) and Vermont (H.764), implemented data protection laws that will contribute to the increasingly complex web of regulatory requirements.

Given the continuous evolution of cyber threats and data protection laws, due diligence investigations should go beyond a narrow review of a target's cybersecurity program and its compliance with data protection laws, and focus on the target's overall culture of security and privacy. The target may not be currently violating any laws, but does it have the institutional framework in place to recognize new regulatory requirements and adjust its policies and procedures accordingly? Does the target have an information governance structure? If so, is that structure capable of effecting meaningful change in response to additional rules and regulations? Has the target's leadership set the proper tone in dealing with security and privacy issues? Organizations with internal information governance structures are better able to adapt to changes in data protection laws, and to mitigate the monetary and reputational costs attached to noncompliance.

Lastly, post-closing compliance mitigation measures should focus not just on short-term issues, but on building the information governance structures of target companies to mitigate the risks posed by both cyber threats and regulatory agencies that are willing and able to enforce new and comprehensive data protection laws.

Please contact Steve Stransky, Mike Ragan or Tony Kuhel for more information.

Employment Compliance in Government Contracting

A complimentary webinar series for HR professionals, corporate legal counsel, and procurement, contracting and compliance personnel

We are pleased to present a series of hour-long webinars examining the unique employment-related compliance requirements faced by federal government contractors and subcontractors, including affirmative action, prevailing wages and benefits, paid sick leave, and recordkeeping and reporting. We will also discuss the current efforts of the U.S. Department of Labor to monitor and enforce all aspects of a government contractor's employment compliance obligations.

All webinars will be held from 1:00 to 2:00 p.m. EDT. Click the link(s) below for more information or to register; you must register for each session individually.

- **Thursday, June 6** – Pay Equity Audits: What, Why, How: More details | Register
- **Thursday, July 18** – Mid-Year Compliance Check: More details | Register
- **Thursday, September 26** – Prevailing Wages, Benefits and Leave: More details | Register
- **Thursday, December 5** – End-of-Year Wrap-Up and Look Ahead for 2020: More details | Register

After you register, you will receive a confirmation email containing the webinar log-in information.

Questions? Contact Stacy Weiner, 202.263.4184, Stacy.Weiner@ThompsonHine.com

Conflicts of Interest

Lessons Learned from Government Contractors: Compliance with Conflict of Interest Laws

By Tom Mason and Francis E. Purcell, Jr.

You might ask, what does a government contract have to do with my business? Or, you may think, we do not conduct any business with the United States or any other state or local government, so why should we care about regulations that require certain clauses be included in contracts governing the delivery of goods and services under a government contract? The Federal Acquisition Regulation, known as the "FAR," provides regulatory guidance that becomes binding when this guidance becomes a term of a contract. The FAR, however, provides more than just regulatory guidance. It often reflects corporate best practices.

In this short article, we will address the importance of avoiding or mitigating organizational and personal conflicts of interest. As we consider avoiding conflicts of interest, we will introduce the FAR's approach to this important subject. The avoidance and mitigation of conflicts of interest saves time, money and needless litigation while enhancing company productivity and employee morale. Moreover, the avoidance or mitigation of conflicts of interest ultimately increases competitiveness while building strong brand recognition and customer acceptance and loyalty.

Organizational Conflicts of Interest (OCI) Must Be Avoided or Mitigated

The FAR requires that corporations doing business with the United States avoid conflicts of interest. There are two broad types of conflicts that must be avoided: organizational conflicts of interest (OCIs) and personal conflicts of interest (PCIs). (See Section 9.504, Section 52.203-16 and Subpart 3.1106 of the Federal Acquisition Regulation.)

An OCI occurs when contracting corporations gain an unfair competitive advantage when contract specifications or award criteria are biased in favor of one or more competitors, when competitors are afforded unequal access to information and/or when the objectivity of an acquisition decision-maker is impaired.

To ensure that government contracts are awarded fairly, the FAR requires contracting officers to avoid, neutralize or mitigate potential significant OCIs. This requires ongoing diligence. More importantly, the FAR requires the contractor to prepare an OCI Avoidance and Mitigation Plan which is incorporated into the contract as a performance requirement.

Personal Conflicts of Interest Must Be Avoided or Mitigated

Likewise, the FAR provides guidance on personal conflicts of interest (PCIs). Personal conflicts of interest arise when an employee relies upon proprietary information regarding another entity's processes, personal relationships or, as is sometimes the case, the employee has a relationship with a member of the contract award selection team or other individual who can provide contract competitive information. Like OCIs, PCIs must be avoided or mitigated by conducting thorough due diligence and by assigning employees tasks that will avoid a PCI.

A PCI often arises when a corporation hires an employee from another entity to take advantage of the employee's knowledge, experience and hoped-for insight stemming from the employee's past experience. While past performance and experience are permitted, any effort to gain access to information that will create a conflict must be abandoned. Because experience and knowledge gained from prior employment is invaluable, great care must be taken to protect trade secrets, proprietary processes and other business proprietary information. While the government will issue a "Post Employment Letter" for each departing employee outlining areas where the employee may work without conflict, private companies often do not provide such letters, making diligence essential. Nondisclosure agreements used to protect confidential and proprietary information are also essential, but these should not replace effective ongoing diligence.

Resolving Conflicts Is the Responsibility of All Parties to a Contract

Following the FAR model, each party to a contract is responsible for avoiding and mitigating conflicts of interest.

While the government defines its proprietary information as tasks that are classified as inherently governmental functions, every employer must consider that any employee who operates and/or supports an employer's acquisition practices, policies and processes, or is knowledgeable about product pricing and delivery, is exposed to proprietary information that must be protected as the release of this information likely would create a conflict of interest. Since it is likely that contractor employees will continue to be highly sought after due to their significant and relevant experience, corporate leaders must ensure that conflicts are avoided or mitigated.

The Need for Corporate Conflict of Interest Policy

There is a great need for every corporation to develop a plan to deal with conflicts of interest. In the best case, conflicts create only an "appearance" of a conflict and steps can be taken to avoid or mitigate the apparent conflict. In the worst case, product development, selection of subcontractors, contract and subcontract awards and contract administrative decisions result from improper influence, and the shareholders/stakeholders believe that they have been defrauded. The policies outlined in the FAR operate to bring about a "best case" outcome in every instance. When OCIs are avoided or mitigated, neither the contract award process nor contract performance are impaired. These conflict of interest policies often free up more time for companies to develop products, delivery systems and unique pricing strategies. Moreover, the implementation of shared responsibility whereby all company personnel have a role in the identification and mitigation of all conflicts of interest is essential. Following the example required by the FAR, corporations should prepare a unique plan to identify, avoid or mitigate conflicts to facilitate the elimination of conflicts. All employees should be required to comply with this plan. This in turn will lead to a favorable working environment whereby corporate resources can be applied to product development, enhanced service offerings and higher compensation for employees for services offered and/or supported. The emphasis and focus on business development, without relying upon the proprietary data of a competitor, creates a positive culture.

Reporting Conflicts of Interest

A corporation benefits when it has avoided all conflicts of interest. The expense in dealing with unmitigated conflicts is far greater than the expense associated with enacting and following a policy that requires the identification and avoidance of any conflict of interest. The first step in becoming conflict of interest free is to ensure that effective training is conducted and every member of the company is encouraged to report any potential conflict of interest. It is required by the FAR and should be a requirement in every corporate employee handbook. Avoidance and mitigation starts with the identification of a potential or likely conflict. Company hotlines may be employed to ensure that all potential conflicts can be reported, investigated and resolved. Recently, after delivering a speech about avoiding and mitigating conflicts of interest, an individual approached and offered the following scenario. The individual claimed to own an invention of a product – a tool – which was sold by the individual's current employer. This employee had conceived and obtained a patent for this tool prior to joining the company. The individual was receiving royalty payments each time the patented tool was purchased. Since joining the new company, the individual's receipt of royalty payments continued. The individual mused and observed the existence of an apparent PCI and offered that to any observer the individual's objectivity might be impaired, were this individual tasked to make decisions regarding the purchase of this tool. As the conversation closed, this individual believed that while the tool set the industry standard, the individual's role in purchasing this tool created an apparent conflict and a corresponding need to report this apparent conflict to the company. A slight modification to the employee's duty was all that was needed to avoid the conflict. In this case, and in every other case, it makes sound business sense to report the actual or apparent conflict so that it can be avoided or mitigated.

Company Benefits

The Federal Acquisition Regulation provides clear guidance with respect to the avoidance of conflicts of interest. The duty to avoid or mitigate any potential significant conflict of interest should be required of all employees. Regular training will be required. As we outlined above, a conflict of interest policy is not only an effective regulatory tool under the Federal Acquisition Regulation, but it provides the basis

for the establishment of a corporate best practice to avoid unnecessary litigation, employee discipline, improper hires and other such events that create unplanned turmoil and expense. Alternatively, by adopting and following the practice required by the FAR, corporations can avoid the aforementioned perils and develop proprietary practices that are unique to the company and products that are the proprietary property of the company, while improving profitability and employee morale. The FAR may be difficult to understand and hard to implement, but in the area of avoiding and mitigating conflicts of interest, there is much to take away, consider and apply.

Please contact Tom Mason or Chip Purcell with any questions.

SmarTrade 2019:
International Trade Compliance and Enforcement

Tuesday, May 14 – Cleveland

Thursday, May 16 – Cincinnati

8:30 - 9 a.m. Registration | **9 a.m. - 1 p.m.** Program and Lunch

Please join us for SmarTrade 2019, a complimentary, informative and interactive workshop focusing on risks and opportunities in the regulation of global trade. The workshop format will provide a unique opportunity to discuss industry best practices and common compliance pitfalls with experts in the field and your peers.

Partners Samir D. Varma and Norman A. Bloch will discuss the current compliance and enforcement environment for imports, exports, anti-bribery regulations and associated compliance challenges, and solutions by analyzing the international supply chain issues and global sales activity of a hypothetical company. Through this vehicle, we'll suggest ways to manage your company's risk exposure, and provide practical tips for dealing with government investigations relating to global trade transactions. Finally, we will discuss the current administration's approach to international trade and its impact on U.S. businesses.

Topics:

- Avoiding violations of U.S. export controls or economic sanctions
- Avoiding violations of anti-bribery laws, including the U.S. Foreign Corrupt Practices Act (FCPA) and the UK Bribery Act
- Staying ahead of Customs & Border Protection enforcement, and using knowledge of Customs regulations to reduce costs and audit risks
- Assessing and managing the risks of trade regulatory violations, including civil and criminal penalties
- Preparing your company for government investigations, audits and verifications before the knock on the door
- Conducting internal investigations and submitting voluntary/prior disclosures
- Understanding the roles that OFAC (Treasury), BIS (Commerce), DDTC (State), CBP (Homeland Security), DOJ (Justice) and other government agencies play in the export/import regulatory and enforcement process
- Assessing and addressing individual liability in government enforcement investigations
- Keeping pace with changes in U.S. economic sanctions affecting trade with countries such as Russia, Cuba, Iran, Venezuela and North Korea

To register, please contact Stacy Weiner at Stacy.Weiner@ThompsonHine.com or 202.263.4184.

Trademarks

Trademark Registration Protection for Global Brand Expansion and for Maximizing Company Goodwill and Asset Valuations

By Roger H. Bora

This article summarizes how U.S. and global trademark rights are created and the importance of trademark registration for national and global brand expansion. For ease of reading, "trademarks and service marks" are both referred to as "trademarks" and "products and services" are both referred to as "products."

Introduction

U.S. brand owners should register their trademarks with the U.S. Patent and Trademark Office (USPTO) to receive the full protection of U.S. trademark laws, and because failure to do so may restrict future geographic expansion of branded products.

Companies conducting international business should also seek trademark registration in countries where they do business because the **majority of countries** do not recognize trademark rights absent a country trademark registration, except under rare circumstances. Accordingly, even if companies have used their marks for many years globally without registration, the majority of countries will not recognize that use as creating any trademark rights.

Those issues may limit a company's ability to expand nationally and internationally and may present serious concerns during a sale of a company or company's assets, and may affect purchase price, since buyers expect sellers to adequately protect their intellectual property in countries within which they conduct business and are not eager to buy uncertainty.

How Are Trademark Rights Created?

There are two primary ways in which trademark rights are created globally:

- **"First to file"** principle: meaning whoever files a trademark application first, and secures trademark registration, is generally considered the trademark owner of the registered mark for the listed products in the **majority of countries**.
    - Accordingly, trademark registrations should be viewed as "government-issued business licenses" that grant prima facie trademark rights.
- **"First to use"** principle: meaning whoever uses a mark first is typically considered the owner of the mark for the associated products (assuming there are no earlier-filed trademark applications), but **only** in the **geographic regions** within which the mark is **actually used** – leaving open other geographic regions for other parties to create rights in the same or a confusingly similar mark, which may block both parties from freely expanding their brands nationally.
    - Accordingly, obtaining trademark registration in **first to use** countries is recommended for securing future geographic expansion rights, as well as for other valuable rights.

Brand owners must understand that their U.S., or home country, trademark rights and registrations typically **do not** provide any trademark rights in other countries, since trademark rights are country specific.

Global Trademark Registration and Strategy Considerations

Brand owners should prepare laser-focused filing strategies based upon core trademarks, core products and key countries and avoid the "reactive strategy" – one that responds to "emergencies" to the detriment of protecting

the core marks and products, while exhausting the annual budget. Companies must make difficult decisions regarding which of their trademarks and products to protect and where to protect them and review their filing strategies periodically and modify them, as necessary.

Trademarks should be prioritized based on "value," which may include the following factors:

- **First tier**: includes house marks and major product names used in all markets.
- **Second tier**: includes important product names used in all markets.
- **Third tier**: includes important names used in certain regions, and sub-brands.
- **Fourth tier**: includes slogans.

Core products should be identified and may be prioritized based upon their value to the company and company revenues.

As for country selection, companies should focus initially on top-tier countries, which may include where the:

- Majority of sales take place.
- Key customers are located.
- Distributors/licensees are located.
- Manufacturing takes place.

Clearance

Once the key marks, products and countries have been identified, the next step is to conduct trademark clearance searches. The searches should assess the risks of infringing third party marks and whether any third party marks and/or registrations may block the use and registration of a trademark in selected countries.

The searches should reveal whether proposed marks are distinctive (i.e., they function as source identifiers) and whether there are any cultural and/or connotation issues that may require modification of marks.

International Treaties and Laws

There are several key international treaties and laws that companies should consider when preparing trademark filing strategies, including the Madrid Protocol, European Union Trademark system and Paris Convention for the Protection of Industrial Property.

Madrid Protocol

A Madrid Protocol application, also referred to as an International Trademark Application and ultimately an International Registration (aka an "IR"), is an international trademark application that is filed through the applicant's home country trademark office, which is the USPTO for most U.S. companies, that allows brand owners to file trademark applications in multiple countries via one application filing. To qualify for a Madrid Protocol application filing, however, the applicant must rely upon at least one home country trademark filing that forms the basis for the Madrid filing.

Once filed, the USPTO reviews a Madrid Protocol application and, if it meets filing requirements, forwards it to the World Intellectual Property Organization (WIPO). The WIPO then reviews the application and, if it meets WIPO's minimum filing requirements, forwards it to each of the ***designated*** country trademark offices.

For example, if a U.S. trademark owner designates the EU, India, Mexico and UK in a Madrid application, the WIPO essentially "files" those applications on behalf of the trademark owner in each of the designated country trademark offices. Just like anything else, however, the Madrid Protocol has advantages and disadvantages.

Advantages include:

- Lower initial filing costs vs. national application filings – savings can exceed 40 percent!
- May currently select up to 119 countries (80 percent of global trade) in one Madrid filing.
- May continue to designate additional countries in the same registration.

Disadvantages include:

- A Madrid filing and **all** designated country filings are **dependent** upon the underlying trademark filing(s) for the first **five years** of the IR. Therefore, if the underlying trademark filing(s) expire within that five-year period, all designated country filings would also fail.

For those reasons, companies should consider the practicality of using the Madrid Protocol strategy and not focus only on cost savings … no matter how enticing they may be.

European Union Trademark (EUTM)

The EUTM trademark registration covers all EU member countries in a single trademark application.

Advantages include:

- **One** application covers **all** EU member countries, with **one** filing fee and **one** renewal fee.
- EUTM registration covering all EU member countries may be less expensive than filing two or three separate country applications.

Disadvantages include:

- EUTM trademark registrations are either "good to all" EU member countries or "good to none." Meaning if there are parties with prior rights in **any** EU member country and should a party successfully object to the EUTM filing, the EUTM filing would fail.

Paris Convention for the Protection of Industrial Property

The Paris Convention is an international treaty that allows trademark applicants a six-month priority period within which to file subsequent foreign trademark applications and receive the same priority filing dates as listed in their first-filed applications.

Companies should utilize this powerful tool when undertaking a global trademark filing strategy, which allows brand owners to spread out costs over the six-month priority period while maintaining the earliest possible priority filing date in key countries.

International Trademark Filing Strategies

Once brand owners identify their core marks and products, select the primary countries of interest, identify members of the Madrid Protocol and European Union (if EU countries are contemplated) as well as any other relevant country pacts, they are ready to formalize their trademark application filing strategies.

As a next step, brand owners should undertake a cost estimate review for the selected countries. A filing strategy may consist of a one to three year (or more) "rolling" filing strategy, depending upon budget, and spreading out the costs, including during the six-month priority period.

How should companies proceed with trademark protection? Should they use the Madrid Protocol? European Union trademark filing? National filings? Or possibly all three?

Companies should consider the risks of using the Madrid Protocol and EUTM filings, including the risks listed above, and prepare the filing strategy based upon those risks, practical business factors and budget.

As you can see, there are many filing considerations and options for seeking global trademark registration protection. Brand owners that fail to implement a well-crafted and coherent global trademark strategy will likely find that they have failed to maximize brand protection and asset valuations, possess inadequate trademark protection for key brands and products in key markets, have not minimized business and infringement risks and consistently run over budget.

Please contact Roger Bora with any questions.

Patents

An Overview of the Process for Obtaining a Patent

By Larry D. Williams Jr., Ph.D.

A typical patent application is a significant investment for any size organization trying to protect its intellectual property. Preparing an application directed to an invention of moderate complexity may cost tens of thousands of dollars, and that is just to produce an application suitable for initial filing. At least three people are typically involved with drafting the patent application on behalf of larger organizations: the inventor, in-house patent counsel and outside counsel. Despite usually not knowing the full contours of their clients' total legal budget, outside counsel understand that patents often represent the largest line item in the budget, and they also understand that this line item is facing increasing scrutiny by the upper levels of many organizations' managers. In-house patent counsel occupies a critical station for coordinating the efforts of the inventor and the outside counsel to minimize inefficiencies in the patent drafting process. This article, the first of two planned articles, provides an overview of the patent application process.

The patent application process begins when the inventor has created a mostly finished product that includes an inventive feature. After creating her invention, the inventor must now disclose it through descriptive writings and drawings. Ideally, the inventor's organization provides a standard disclosure form to solicit a uniform type and amount of disclosure from its inventors. These forms may be customized for each organization's needs, and outside counsel often help draft them or review drafts prepared in-house. Typical information collected by the form includes: (1) inventor information, such as name, address and citizenship; (2) description of background art; (3) identification of the problem solved by the invention; and (4) a detailed description of the inventor's solution to that problem.

Once the inventor submits the disclosure to the appropriate person or department, many organizations have mechanisms for evaluating the disclosure to determine if the patent process should continue. Many factors should be weighed in making this decision, such as the potential impact on the organization if the invention is patented or is not patented, the feasibility of producing a product in accordance with the disclosure, the defensive potential of a granted patent (or even the pending patent application), and the offensive potential of a granted patent if a competitor does enter the market with a product covered by the patent. Additional factors may be pertinent, and in-house patent counsel, business leaders and, potentially, outside counsel may work together to identify such factors.

Assuming the organization decides to move forward with the patent application, it will either be drafted completely in-house or by outside counsel. The main advantage of drafting a patent application completely in-house is decreased initial legal fees. However, the disadvantage is that disputes may arise between the inventor, who is not often a patent expert and so may not appreciate the broader inventive aspect embodied in the inventor's work, and in-house counsel, who wants to protect as much of the patent landscape as possible within the confines of the prior art. In effect, outside counsel can act as a neutral third party who helps protect the relationship between in-house counsel and inventor. Additionally, patent drafting takes a large amount of time, even when performed completely efficiently. In-house counsel simply may not have the amount of time required.

In either event, the next step requires that someone other than the inventor understand the invention so that a first draft of the claims may be produced. Entire treatises are devoted to invention claiming, and this topic is beyond the scope of this article. Simply stated, the claims should be broad enough that a competitor cannot easily design around them while narrow enough that they are definite and do not read on the prior art. The inventor typically discloses one or two embodiments of the invention in the disclosure form, but the inventive concept may be much broader than those embodiments. The patent drafter is tasked with encouraging the inventor to think bigger lest the claims become too narrow and of minimal value. Often the inventor is receptive toward the drafter's recommendations, but sometimes she is not.

At this point, the drafter may ask the inventor to review the claims before drafting the specification, or he may instead simply begin drafting the specification. The specification has many attributes in common with peer-reviewed technical literature, but at its core, a patent application is a legal document and must be drafted as such. Based on decades of patent case law, there are many words and phrases that should never appear in any specification, and the drafter will keep these words and phrases in mind when drafting the specification. An engaged inventor is critical at this stage to ensure that the document fully describes the invention such that one of ordinary skill in the art can make and use the invention without undue experimentation. Patent application drafting is a team event, and one or more drafts may be produced, distributed and revised before the completed application is ready for filing.

The completed application is then filed at the United States Patent and Trademark Office, where it will undergo a formal review by a technically trained patent examiner. The patent examiner and patent attorney will exchange letters, potentially many rounds of letters, in which a type of negotiation takes place. The examiner often views his role as protecting the public from losing control over technology that was already in the public domain, and the patent attorney views his role as securing rights to technology that was not in the public domain for the initial creator of that technology. If all goes well, the application will issue as a patent, giving the owner of the patent the right to exclude others from making, using or importing the technology for a limited period of time. A patent typically issues several years after filing the application.

The patent application process is long and fraught with chances for inefficiency to creep in. Part II of this article will describe typical sources of inefficiency in the patent drafting phase and provide suggestions for minimizing these inefficiencies.

Please contact Larry Williams with any questions.

Employment & Benefits Law Briefing – Seven Key Internal Audits

Tuesday, May 21 – Cincinnati

8:00 – 8:30 a.m. Registration & Continental Breakfast | **8:30 – 11:35 a.m.** Program

Please join us for an informative breakfast briefing designed for in-house counsel and human resources professionals. Members of our Labor & Employment and Employee Benefits practices will address internal audits your company should consider conducting in seven critical areas, particularly with regard to recent regulatory developments, litigation trends and heightened enforcement scrutiny in certain areas.

Our topics will include:

- Auditing Your Pay Practices: Heather Muzumdar
- Auditing Your Dispute Resolution Policy: Steve Richey
- Auditing Your Workplace Investigation Procedures: Deborah Brenneman and Lindsay Nichols
- Auditing Your Leave Policies: Megan Glowacki
- Auditing Your Employee Benefit Plans: Erin Shick
- Auditing Your Immigration Policies and Practices: Staci Jenkins
- Auditing Your Policies for Employees and Contractors: Scott Young

Attendance is complimentary, but please register online by May 17. CLE and HRCI credit has been requested.