Business Law Update August 2014

PUBLISHED ON

August 1, 2014

TABLE OF CONTENTS

What's in a Name? Why Business Names Matter

By: Scott F. Landis and John T. Reed

What's in a name? That which we call a rose
By any other name would smell as sweet
-William Shakespeare, *Romeo and Juliet*

In the above quote from Romeo and Juliet's famous balcony scene, Juliet is arguing that the names of things really do not matter. Of course, when it comes to names for your business, you know that names do in fact matter very much. For example, you file a name with the Pennsylvania Department of State, get confirmation of the filing from the State, order signs for your building, letterhead, business cards, etc. and start advertising your business. Then, two months later you get a very formal looking letter from a lawyer saying you have no right to use your name and you must immediately stop. Wait, that cannot happen, right? The State said you could use the name. Unfortunately, it can and does happen. Depending on what you are using the entity for, the name can be one of the most valuable assets of the business, and confirmation from the State that the name is available is just one part of protecting that asset. Below, we will discuss three types of names for your business and what you get and do not get from each; 1) legal or entity names; 2) trademarks (including service marks); and 3) domain names.

Legal or Entity Names

Your legal or entity name is the official name under which your business entity (e.g. corporation, limited partnership, or limited liability company) is registered with the state. Your business' legal name is the name that appears on contracts, tax returns, and other legal filings. No two entities registered in a particular state can share the identical or nearly identical name. Before settling on an entity name, therefore, the availability of that name needs to be confirmed with the appropriate office of the state where your entity is incorporated or registered. In most cases, this office is a division of the department of state or the department of revenue. However, as described above, the State allowing you to form the entity does not mean you have the right to use that name in commerce. If another person or entity is already using that name or a similar name, they may be able to prohibit you from using it. So, if your intention is to use the name in commerce, making sure the name is available for State filing is just one step in the process.

Trademarks & Service Marks

Trademarks & Service Marks identify and distinguish a particular product (trademark) or service (service mark). In addition to names, trademarks and service marks can include logos, symbols, sounds, colors, slogans, or anything else that functions to distinguish your products and/or services from those of your competitors. Trademarks and service marks differ from entity names in several significant ways. First, a trademark or service mark does not need to be registered. In the United States, trademarks or service marks come about from the use of the mark in commerce. This type of protection is called common law protection. Although not required, trademarks and service marks can be registered with the United States Patent and Trademark Office. If the name is important and will be an asset, a clearance search will allow you to determine if someone else is using the same name or a similar name. If not, while not required, registering such name may be advisable. Registration provides significant advantages to the owner of the mark, including the presumption of validity and right to exclusive use, and the ability to seek increased damages and attorney fees in an action for infringement. Another significant difference between entity names and trademarks or service marks is that businesses can and do have and use identical trademarks/service marks. If the products or services associated with a mark are not sufficiently similar or related as to create a likelihood that consumers will be confused into believing the products/services originate from the same source, then the identical or similar marks can co-exist. An example of this is the mark "Delta" for both airlines and faucets. Here it is not likely that consumers will be confused into believing that the airline is the same company that makes bathroom faucets so there is no conflict. Finally, a trademark or service mark serves a materially different function in your business. Your entity name is the name of your entity. Your trademark or service mark is the name of your product or service. This can sometimes be a subtle distinction, particularly in the case of service marks (e.g. "McDonalds" is a registered service mark for "McDonalds Corporation"). But it is a significant legal distinction nevertheless.

Domain Names

A domain name is the name which identifies the location of your web site on the Internet. The domain name usually consists of a series of letters and/or numbers followed by a top level domain (.com, .net, .info, etc.). Because it identifies a specific Internet location, each domain name must be unique and no two web sites may use the same domain. But businesses can, and do, have multiple domain names. Many companies will have a domain name that is identical or similar to their entity name or to one or more of their trademarks or service marks. The nature of domain names has created many opportunities for conflict. More than one company may have rights to use the same trademark or service mark, but only one of those companies can have the equivalent domain name. Your competitor, or another party, may attempt to register a domain name similar to your name for the purpose of keeping you from registering it, or in an effort to sell it to you for an inflated price. Of course because there are hundreds of different top level domains, with more likely on the way, it is not practical for most businesses to register each and every possible domain name variation of your name. But businesses should still be attuned to the potential issues here.

Protecting and Clearing Names

By now you hopefully understand that just because you are able to use a particular entity name, that fact by itself does not mean you will be able to use a particular trademark, service mark, or domain name, and vice-versa. Therefore before you settle on a name for your business, it is important that you check the availability for the name from an entity name, trademark/service mark, and domain name perspective. The most reliable way to do this is to commission a full clearance search and review by an experienced attorney. Once a name is determined to be available, proper entity and domain name registrations should be filed. Federal registration of trademarks and service marks should also be strongly considered. Taking these relatively simple and inexpensive steps from the outset can save you from the grief and despair of finding out that your name is not fully available after you have spent money and time promoting it.

Back To Top

Market Entry Strategies: Should Your Business Enter a New Market Directly, Via a License Agreement, or thr

Is your business growing? Do you plan on exploring opportunities in new product lines or previously untapped markets? Businesses often pursue expansion opportunities, and a key element to any company's success is effective growth management. Whether your business is expanding its reach domestically or entering into a new foreign market, a fundamental question is what type of vehicle your business should use to best achieve its market entry objectives. Considerations related to corporate structure, risk management and investment goals are central to formulating an effective market entry strategy. While this article will focus on the decision points relevant to entering a foreign market, many of the principles discussed herein are equally applicable to various domestic expansion scenarios, such as, entering a new product / service market or selling existing products in a previously untapped region of the country. This article will begin with a discussion of some general considerations related to operating in a foreign jurisdiction and will then highlight three common market entry strategies: 1) direct presence; 2) licensing agreements; or 3) a joint venture.

The Foreign Market: Key Considerations

Expanding your business into a foreign jurisdiction entails substantial and sometimes unforeseen operational costs. Foreign countries may have vastly different legal systems, economic structures and social constructs. All of this creates uncertainty which complicates market entry. Thus, a cost-benefit analysis (including market potential) is an important first step prior to entering any foreign market. Similar to the case of a domestic merger or asset acquisition, it is important to conduct thorough due diligence on any potential foreign market.

When considering market entry strategies, some important initial considerations include:

- Production. Does entry into the market require that any goods sold actually be produced in the foreign market, or is importing an option? In addition, are any other import/export restrictions applicable (including as to technology)? Does production capability already exist in the market? Is a local "partner" available?

- Distributors and/or Sales Agents. Can market entry be accomplished through distributors or sales agents?

• Foreign Investment / Local Ownership Controls. Are there any legal restrictions on foreign "inbound" investment in the new market (or local ownership percentage requirements)?

• Personnel issues. Operating in a foreign market, regardless of the form, will present employment issues such as: travel, hiring and/or personnel transfer (immigration).

• Professional Advisors. Entry into a foreign market will generally require the advice of suitable professional advisors in the new market (i.e., legal, accounting, QA/RA, etc).

• Culture. Have cultural, religious and language differences been examined to identify any non-legal barriers to product entry and success in the target market?

• Miscellaneous. Are other legal or non-legal issues presented? Some potential issues are: antitrust/unfair competition; cross-border taxation; or accounting.

• Exit strategy (monetizing the new venture). Consider the means of exit under both good and bad circumstances.

The aforementioned considerations regarding foreign market conditions, when coupled with an analysis of the market entrant's specific goals, are crucial to determining which market entry structure is preferable. These factors can all significantly impact the level of risk and financial investment required to effectively enter a new market.

Market Entry Strategies: Specific Options

Direct Market Entry

One possible market entry strategy is to form a corporate presence in the foreign jurisdiction and to acquire market production capacity (including any required intellectual property rights and regulatory authorizations). Direct market entry is most commonly accomplished by either merging/acquiring a previously established company in the jurisdiction, or forming a new wholly owned operational entity in the target locality. Direct participation can be simpler from a management and operational perspective. Unlike the license agreement or the joint venture, the success of direct participation is not dependant on cooperation with a local "partner" (see below). Direct market entry therefore allows for a high level of control, but also requires significant up-front investment, particularly considering that start-up costs in a new jurisdiction can often be rather high (from both a personnel and financial standpoint). As there is no "partner," it is important to note that in some jurisdictions, direct participation in a foreign market may be hampered by laws limiting foreign investment or requiring that a stated percentage of the entity be locally owned (local ownership requirements).

License or Joint Venture?

As an alternative to direct entry, two common market entry strategies are to license specific intellectual property to a local affiliate (generally in exchange for royalties) or partnering with a local affiliate to produce and/or sell the products in the foreign jurisdiction (a joint venture).

In the context of intellectual property ("**IP**") law, a "license" is a grant from the owner of an IP right (the "**licensor**") to another entity (the "**licensee**") permitting the licensee to make certain uses of the IP, for example, to distribute products under the licensor's trademark or manufacture products using the licensor's patent protected process, trade secrets or know how.

A joint venture generally involves a commercial collaboration between two or more independent entities, formed for either a single purpose project or a continuing business. Joint ventures can be formed: (i) as new entities, jointly owned or owned in an agreed proportion by the joint venture parties; (ii) when one party buys an interest in an existing entity's start-up or developing business; or (iii) through a contractual relationship without the use of a separate entity (sometimes referred to as alliances or strategic alliances).

Comparison of a License and a Joint Venture

License: As a general rule, licensing or other transfers of IP/technology entail less costs and difficulty than a joint venture, but also generate less financial return than actually "making" the product in the market (license agreements generally provide for a "royalty fee," which is often either a flat annual fee or a stated percentage of sales). A licensing agreement usually enables a firm to enter a foreign market quickly, and poses fewer financial and legal risks than owning and operating a foreign manufacturing facility or participating in an overseas joint venture. This is because licensing rarely requires significant levels of capital investment and does not require that the parties work closely together or demand continuous attention. Licensing also permits U.S. firms to overcome many of the tariff and nontariff barriers that frequently hamper the export of U.S. manufactured products.

There are also various drawbacks to a license in addition to the reduced profits. For instance, the licensor has reduced control over the product quality, distribution and marketing policies. The licensor will also have less control over the essential support services personnel employed for the purpose of manufacturing/selling the product or technology. Furthermore, if consideration is based on sales volume, the licensor must rely on the honesty of the licensee to report units sold.

Joint Venture: Joint ventures often involve additional costs and expense, but allow for both greater control and greater potential profits. As noted above, the income on a license agreement is usually limited in some way (a royalty based on a percentage of sales, etc). This is not the case for a joint venture, although the parties may agree to split any profits however they see fit. In addition, an international joint venture enables a firm to actually establish a marketing or manufacturing presence abroad with the assistance of a local foreign partner (whereas as licensor would generally have a much more limited presence in the new territory). The local partner may also provide added value through their knowledge of government workings, regulations, internal markets and distribution know-how. This knowledge may be particularly valuable in an unfamiliar or volatile region.

Additionally, a number of potential disadvantages are associated with a joint venture. A joint venture will likely require a greater investment than a license agreement (in both time and resources). Moreover, when compared to a license, there are additional risks inherent to a joint venture as they require significant levels ongoing cooperation between the parties and a greater presence in the foreign country. For example, if a disagreement or dispute between the parties results in reduced operational control, the U.S. company may experience reduced profits, increased operating costs, inferior product quality, exposure to product liability, and environmental litigation and fines. U.S. firms that wish to retain effective managerial control will find this issue important in negotiations with the prospective joint venture partner.

Thus, a choice between a license and joint venture will often turn on issues such as a potential market entrant's level of risk aversion and expectations regarding inter-entity cooperation, up-front investment costs, and profit margins.

Selecting a Partner

Regardless of whether a license agreement or a joint venture is selected as the appropriate vehicle, it is generally necessary to "partner" with another entity, although the level of cooperation varies depending on the specific type of market entry strategy and the scope of operations. Thus, selection of an appropriate "partner" is important, whether they are a licensee, partner, investor, etc. Selection of a partner is especially important with regards to considerations of quality control and regulatory compliance, both critical needs that will be fulfilled at the foreign location.

Deficiencies in any of the areas identified below would suggest that a potential "partner" must be examined with extraordinary care:

• Are the market entrant and the potential partner "culturally compatible" (both in terms of corporate culture and foreign social culture)?

• How does the potential partner, and its business operations, fit within the market entrant's overall strategic plan?

• What is the reputation of the potential partner within the foreign market generally and the specific industry (i.e., among customers, suppliers, regulators, and/or consumers)?

• What is the potential partner's organizational (i.e., management) level of skill and sophistication? What support financially and logistically will the potential partner require?

• What are the financial resources of the potential partner? Do they have sufficient access to capital? Is there any danger of insolvency?

• What financial reporting standards are applicable to the potential partner? Are third parties available to confirm compliance?

• With respect to IP, does the potential partner have sufficient technical and operational skill?

• If applicable, what is the potential partner's prior history with respect to the use or licensing of IP? Has it been involved in any previous litigations which involved claims of misappropriation of IP?

• Does the potential partner have sufficient manufacturing, distribution, and logistical experience?

• What is the potential partner's sales/marketing experience and capabilities?

• What is the potential partner's regulatory compliance capabilities and history?

• Technology Transfer

• The final issue to be considered are questions regarding technology (IP) transfer. As IP laws can differ based on the jurisdiction, entry into a foreign market may pose various risks related to an entrant's IP rights. Consequently, whether a license or joint venture is used to enter a foreign market, it is critically important to protect (i.e., prevent the exploitation of) any IP rights licensed or contributed to a joint venture vehicle.

• A potential market entrant should carefully consider each of the following questions in order to best protect its IP / trade secrets and maximize its return on investment:

• (a) If technology (as opposed to trademarks or names) is to be transferred:

• (i) Is the IP patented in the U.S.? Has the IP been patented in the new market? If not, when will this be possible?

• (ii) How will know-how or trade secrets be protected? It is important to be very careful when considering how the applicable law and other issues in the foreign jurisdiction will impact the protection of specific forms of IP. Poor choices can put key assets at risk.

• (iii) Pricing the transfer. Will a royalty be used or some other approach? Will the royalty be based on a flat fee or a percentage of sales? Will there be a minimum royalty?

• (b) If trademark/name/etc. is to be licensed:

• (i) Have appropriate filings been made in both the U.S. and the foreign jurisdiction? If not, when?

• (ii) Is prior use a requirement for registration in the foreign jurisdiction?

• (c) Is the involvement of key personnel required to complete the transfer? Can they be spared? May their knowledge be legally transferred?

• (d) Despite the legal arrangements, should key aspects of technology or know how remain under trade secret protection?

• (e) May the technology be legally exported/imported?

This article has reviewed various strategies and considerations relevant to operating in a foreign jurisdiction. Not only is it critically important that a business carefully select new markets, but equally important is selecting the proper market entry vehicle (and the selection of a related "partner," if applicable). We have experience advising clients on matters related to direct market entry, licensing agreements, joint ventures and technology transfer, and would welcome the opportunity to discuss any of these matters further.

Back To Top

Contract Risk Management - Looking Beyond the Words On the Page

By: Kimberly J. Decker

Businesses enter into contracts every day as they purchase supplies, sell products and make business deals. Contracts are desirable because they describe the deal that was made and what each party to the contract is required to do. This helps to avoid problems and misunderstandings later. A good contract, however, also describes what happens if the deal goes bad - something you don't want to be caught negotiating after the fact.

If you do not have a form of sales and purchase terms and conditions that have been reviewed by legal counsel, or you do not understand how to use them to your best advantage, this should be your number one contract priority. Cutting and pasting provisions that you think look good from various contracts that you have worked on is **not** a good idea - you will likely end up with legal problems that far exceed the cost of hiring an attorney to do this work in the first place. A little work with a lawyer can help you manage your risks at a relatively low cost by customizing your contracts to address your particular business' risks. However, the legal words are only a portion of managing contract risks.

Managing Contract Risks

Below are the top five reasons why your contracts don't adequately manage your risks:

1. Your sales force does not use your standard forms. Having a standard contract is great, but you have to use it. Starting from your own form almost always gives you an edge, regardless of how much it is negotiated. However, depending on your industry and your bargaining power, there may be times where you have to start from someone else's contract form. When that happens, you should have someone on staff with a lot of contracting experience, or access to a lawyer. Contracts are rarely written in "plain English", and there are plenty of traps for the inexperienced negotiator.

2. Your sales force uses your standard forms, but they readily give away the "legal farm" to make deals happen. This approach will likely create a big headache - and unexpected liability - down the road. We recommend that you provide your sales force with at least basic training on contracts, the meaning of frequently used legal terms and why they are important. However, negotiators also need to also understand where they do - and don't - have authority to bargain. To provide that kind of guidance, we recommend that you identify, as a matter of business policy, what contract terms are:

- Absolutely critical to your business, and non-negotiable
- Important, but you might be willing to negotiate if necessary
- Routine and free to be negotiated

Making these decisions requires both business and legal input. Having this framework in place provides guidance to your sales force, gives consistency to your contractual relationships (almost everyone gets the same deal) and makes your sales force accountable not only for the business deal that they make, but for the legal concessions they may make.

3. Your sales people start from the wrong contract. This typically happens when someone sends out the contract from the last deal they did, which was negotiated, rather than your standard form. Ultimately, if the process of starting from the last deal continues, your contracts will end up offering less and less protection over time - usually, with no one the wiser until it is too late.

4. Contract attachments (often product specifications, pricing formulas and charts, project preparation duties, descriptions of services to be provided and the like) never get attached to the contract or, worse yet, no one can find the final, signed contract. This is often discovered when you already have a problem with the other party, making that situation even more difficult to resolve. Assigning a department or person to manage your contracts and keep track of these details is vital.

5. You have risk-mitigating contract management policies and procedures in place that should keep the above issues from happening, but you don't really enforce them. As a result, over time, your sales people become more and more lax about these policies and end up reverting to their own way of handling negotiations and keeping track of contracts. We recommend that you provide a designated person or department to make decisions about when, and under what terms, you will negotiate contract terms. This

person will help with those negotiations so you are only giving up what you have to in order to get the deal done. The designated person or department should also keep track of contracts, ensure that they are signed, have all exhibits and know when to pursue legal advice.

It is up to every business to decide what resources it is willing and able to devote to contract management. Contract management and its goals need to be supported from the top of the organization in order to be effective. Without the right corporate policies (and support of those policies), your sales people have no incentive to use your form contracts, to negotiate the best legal protection they can or to consult with legal counsel when necessary.

Ultimately, contract administration is just as vital to your business and risk management as the words of the contracts themselves. Good contract administration can ensure that you get the protection you expect from your legal forms, maintain consistency in the way you do business on the legal side, avoid future conflicts with business partners, help your organization keep track of contract expirations and deadlines and show business partners that you are organized and capable right from the start of the relationship.

Back To Top

Compliance Issues Inherent in Bring-Your-Own-Device Programs

Employees use their own smartphones and tablets to perform a variety of work-related tasks. Even in companies that do not explicitly condone the use of personal devices for work use, employees often connect their devices to work systems. This increased use of personal devices in the workplace has brought with it a host of legal issues. Devices containing corporate or personal data can be lost or stolen. Viruses can infect corporate systems. Employees can use their devices to violate policies or company contracts. As a result, many companies have instituted formal bring-your-own-device (BYOD) programs to set expectations and ground rules for use of these devices. While there is no specific "best practice" when it comes to setting rules, this article will provide some basic considerations and strategies.

Security

The biggest risk to companies from BYOD is a potential breach of security. When a device is lost or hacked, not only is the company's own sensitive information at risk, but the loss may also breach confidentiality obligations that the company owes to third parties. Employers may choose to implement mobile device management (MDM) tools to manage risk in this area, including mandatory registration of employee devices, mandatory use of password protection, encryption for data sent through the corporate network, and remote wiping in the event a device is lost. Depending on the sophistication of an IT department, this may also limit the number of supported devices, and employees should obviously be made aware of such limits before purchasing any device.

An effective BYOD policy should also contain clear instructions on what activities are permitted on devices that have access to corporate information systems. Keep in mind that tools such as Siri or other standard smartphone applications retain instructions and information in the cloud for up to two years even if employees are not intentionally backing up to a cloud-based service. In addition, employees may be required to give their passwords over to an Apple store technician or even leave their devices overnight on some occasions. Employers, therefore, may want to take precautions to prevent sensitive information-especially information protected by HIPAA, financial regulations, or other state or federal law-from being downloaded into a device in the first place, or at least ensure that it is walled off from other information. Employers may also set rules limiting access of certain websites, backing up work-related information to cloud-based private services, letting friends or family use work devices, or connecting to work through unsecured wireless networks.

Consent

Consent is a key component to any BYOD program. Employees should understand that employers have the right to access, review, and delete data on their personal devices and that they have no expectation of privacy if they choose to use their devices for work purposes. At the same time, there are limits to what employers can monitor. Federal and state laws prohibit unauthorized access to certain electronically-stored information, including Social Security or driver's license numbers, and other personally identifiable information. Employers must also never install anything on an employee's personal device without first obtaining consent. All notices and requests for consent should be clearly written and should cover all potential needs an employer might have to access data on the device.

Litigation and Discovery

One of the reasons employers may need to gain access to personal devices is to comply with court orders or discovery requests. Organizations cannot object to producing information stored on personal devices on the basis that they have become comingled with an employee's personal information. To the extent possible, employers should adopt procedures to separate work and personal data at the outset, ensuring that work data (and only work data) is periodically backed up.

Other Legal Compliance Issues

This article will not address each and every challenge that might arise from a BYOD program. Nonetheless, beyond the right-of-access issues described above, any BYOD policy should include provisions addressing the following issues:

• Consider the tax consequences of reimbursements for devices, and make sure employees are aware of these consequences.

• Consider who will be responsible for lost or stolen devices and who will be responsible for malware or virus attacks associated with an employee's device. Relatedly, consider what kind of IT support the company will provide to personal devices in the event of malfunction.

• Make clear that policies concerning harassment and discrimination apply equally to conduct over mobile devices.

• Prohibit nonexempt employees from performing work "off the clock." Keep in mind that any work conducted on a personal device counts as "hours worked" for purposes of the Fair Labor Standards Act.

• Review the scope of software licenses before permitting employees to access the software from their personal devices. Some licenses limit access and use to devices owned by the company. By the same token, ensure that employees are not inappropriately using third-party software they download on their own for business use if only noncommercial use is permitted.

• Prepare for an employee's departure from the company. If an employee's device contains sensitive information, obtain advance consent to wipe this information before discharge. Of course, if the employees' device is subject to a legal hold as part of ongoing litigation, preserve any necessary information before wiping the device.

BYOD programs create significant risks for companies and require investment in technology to mitigate those risks. Failure to create clear policies regarding use of personal devices, however, can lead to even bigger risks. Once you have determined the contours of your BYOD plan, we can work with you to draft clear policies and procedures for a successful and efficient program.

Back To Top

Business Law Update

By: Kenneth R. Charette, Kimberly J. Decker, Scott F. Landis and Joshua L. Schwartz

In this issue:

What's in a Name? Why Business Names Matter

By: Scott F. Landis, Esquire

What's in a name? That which we call a rose
By any other name would smell as sweet
-William Shakespeare, *Romeo and Juliet*

In the above quote from Romeo and Juliet's famous balcony scene, Juliet is arguing that the names of things really do not matter. Of course, when it comes to names for your business, you know that names do in fact matter very much. For example, you file a name with the Pennsylvania Department of State, get confirmation of the filing from the State, order signs for your building, letterhead, business cards, etc. and start advertising your business. Then, two months later you get a very formal looking letter from a lawyer saying you have no right to use your name and you must immediately stop. Wait, that cannot happen, right? The State said you could use the name. Unfortunately, it can and does happen. Depending on what you are using the entity for, the name can be one of the most valuable assets of the business, and confirmation from the State that the name is available is just one part of protecting that asset. Below, we will discuss three types of names for your business and what you get and do not get from each; 1) legal or entity names; 2) trademarks (including service marks); and 3) domain names.

Legal or Entity Names

Your legal or entity name is the official name under which your business entity (e.g. corporation, limited partnership, or limited liability company) is registered with the state. Your business' legal name is the name that appears on contracts, tax returns, and other legal filings. No two entities registered in a particular state can share the identical or nearly identical name. Before settling on an entity name, therefore, the availability of that name needs to be confirmed with the appropriate office of the state where your entity is incorporated or registered. In most cases, this office is a division of the department of state or the department of revenue. However, as described above, the State allowing you to form the entity does not mean you have the right to use that name in commerce. If another person or entity is already using that name or a similar name, they may be able to prohibit you from using it. So, if your intention is to use the name in commerce, making sure the name is available for State filing is just one step in the process.

Trademarks & Service Marks

Trademarks & Service Marks identify and distinguish a particular product (trademark) or service (service mark). In addition to names, trademarks and service marks can include logos, symbols, sounds, colors, slogans, or anything else that functions to distinguish your products and/or services from those of your competitors. Trademarks and service marks differ from entity names in several significant ways. First, a trademark or service mark does not need to be registered. In the United States, trademarks or service marks come about from the use of the mark in commerce. This type of protection is called common law protection. Although not required, trademarks and service marks can be registered with the United States Patent and Trademark Office. If the name is important and will be an asset, a clearance search will allow you to determine if someone else is using the same name or a similar name. If not, while not required, registering such name may be advisable. Registration provides significant advantages to the owner of the mark, including the presumption of validity and right to exclusive use, and the ability to seek increased damages and attorney fees in an action for infringement. Another significant difference between entity names and trademarks or service marks is that businesses can and do have and use identical trademarks/service marks. If the products or services associated with a mark are not sufficiently similar or related as to create a likelihood that consumers will be confused into believing the products/services originate from the same source, then the identical or similar marks can co-exist. An example of this is the mark "Delta" for both airlines and faucets. Here it is not likely that consumers will be confused into believing that the airline is the same company that makes bathroom faucets so there is no conflict. Finally, a trademark or service mark serves a materially different function in your business. Your entity name is the name of your entity. Your trademark or service mark is the name of your product or service. This can sometimes be a subtle distinction, particularly in the case of service marks (e.g. "McDonalds" is a registered service mark for "McDonalds Corporation"). But it is a significant legal distinction nevertheless.

Domain Names

A domain name is the name which identifies the location of your web site on the Internet. The domain name usually consists of a series of letters and/or numbers followed by a top level domain (.com, .net, .info, etc.). Because it identifies a specific Internet location, each domain name must be unique and no two web sites may use the same domain. But businesses can, and do, have multiple domain names. Many companies will have a domain name that is identical or similar to their entity name or to one or more of their trademarks or service marks. The nature of domain names has created many opportunities for conflict. More than one company may have rights to use the same trademark or service mark, but only one of those companies can have the equivalent domain name. Your competitor, or another party, may attempt to register a domain name similar to your name for the purpose of keeping you from registering it, or in an effort to sell it to you for an inflated price. Of course because there are hundreds of different top level domains, with more likely on the way, it is not practical for most businesses to register each and every possible domain name variation of your name. But businesses should still be attuned to the potential issues here.

Protecting and Clearing Names

By now you hopefully understand that just because you are able to use a particular entity name, that fact by itself does not mean you will be able to use a particular trademark, service mark, or domain name, and vice-versa. Therefore before you settle on a name for your business, it is important that you check the availability for the name from an entity name, trademark/service mark, and domain name perspective. The most reliable way to do this is to commission a full clearance search and review by an experienced attorney. Once a name is determined to be available, proper entity and domain name registrations should be filed. Federal registration of trademarks and service marks should also be strongly considered. Taking these relatively simple and inexpensive steps from the outset can save you from the grief and despair of finding out that your name is not fully available after you have spent money and time promoting it.

Market Entry Strategies: Should Your Business Enter a New Market Directly, Via a License Agreement, or thr

By: Kenneth R. Charette, Esquire

Is your business growing? Do you plan on exploring opportunities in new product lines or previously untapped markets? Businesses often pursue expansion opportunities, and a key element to any company's success is effective growth management. Whether your business is expanding its reach domestically or entering into a new foreign market, a fundamental question is what type of vehicle your business should use to best achieve its market entry objectives. Considerations related to corporate structure, risk management and investment goals are central to formulating an effective market entry strategy. While this article will focus on the decision points relevant to entering a foreign market, many of the principles discussed herein are equally applicable to various domestic expansion scenarios, such as, entering a new product / service market or selling existing products in a previously untapped region of the country. This article will begin with a discussion of some general considerations related to operating in a foreign jurisdiction and will then highlight three common market entry strategies: 1) direct presence; 2) licensing agreements; or 3) a joint venture.

The Foreign Market: Key Considerations

Expanding your business into a foreign jurisdiction entails substantial and sometimes unforeseen operational costs. Foreign countries may have vastly different legal systems, economic structures and social constructs. All of this creates uncertainty which complicates market entry. Thus, a cost-benefit analysis (including market potential) is an important first step prior to entering any foreign market. Similar to the case of a domestic merger or asset acquisition, it is important to conduct thorough due diligence on any potential foreign market.

When considering market entry strategies, some important initial considerations include:

• Production. Does entry into the market require that any goods sold actually be produced in the foreign market, or is importing an option? In addition, are any other import/export restrictions applicable (including as to technology)? Does production capability already exist in the market? Is a local "partner" available?

• Distributors and/or Sales Agents. Can market entry be accomplished through distributors or sales agents?

• Foreign Investment / Local Ownership Controls. Are there any legal restrictions on foreign "inbound" investment in the new market (or local ownership percentage requirements)?

• Personnel issues. Operating in a foreign market, regardless of the form, will present employment issues such as: travel, hiring and/or personnel transfer (immigration).

• Professional Advisors. Entry into a foreign market will generally require the advice of suitable professional advisors in the new market (i.e., legal, accounting, QA/RA, etc).

• Culture. Have cultural, religious and language differences been examined to identify any non-legal barriers to product entry and success in the target market?

• Miscellaneous. Are other legal or non-legal issues presented? Some potential issues are: antitrust/unfair competition; cross-border taxation; or accounting.

• Exit strategy (monetizing the new venture). Consider the means of exit under both good and bad circumstances.

The aforementioned considerations regarding foreign market conditions, when coupled with an analysis of the market entrant's specific goals, are crucial to determining which market entry structure is preferable. These factors can all significantly impact the level of risk and financial investment required to effectively enter a new market.

Market Entry Strategies: Specific Options

Direct Market Entry

One possible market entry strategy is to form a corporate presence in the foreign jurisdiction and to acquire market production capacity (including any required intellectual property rights and regulatory authorizations). Direct market entry is most commonly accomplished by either merging/acquiring a previously established company in the jurisdiction, or forming a new wholly owned operational entity in the target locality. Direct participation can be simpler from a management and operational perspective. Unlike the license agreement or the joint venture, the success of direct participation is not dependant on cooperation with a local "partner" (see below). Direct market entry therefore allows for a high level of control, but also requires significant up-front investment, particularly considering that start-up costs in a new jurisdiction can often be rather high (from both a personnel and financial standpoint). As there is no "partner," it is important to note that in some jurisdictions, direct participation in a foreign market may be hampered by laws limiting foreign investment or requiring that a stated percentage of the entity be locally owned (local ownership requirements).

License or Joint Venture?

As an alternative to direct entry, two common market entry strategies are to license specific intellectual property to a local affiliate (generally in exchange for royalties) or partnering with a local affiliate to produce and/or sell the products in the foreign jurisdiction (a joint venture).

In the context of intellectual property ("**IP**") law, a "license" is a grant from the owner of an IP right (the " **licensor**") to another entity (the "**licensee**") permitting the licensee to make certain uses of the IP, for example, to distribute products under the licensor's trademark or manufacture products using the licensor's patent protected process, trade secrets or know how.

A joint venture generally involves a commercial collaboration between two or more independent entities, formed for either a single purpose project or a continuing business. Joint ventures can be formed: (i) as new entities, jointly owned or owned in an agreed proportion by the joint venture parties; (ii) when one party buys an interest in an existing entity's start-up or developing business; or (iii) through a contractual relationship without the use of a separate entity (sometimes referred to as alliances or strategic alliances).

Comparison of a License and a Joint Venture

License: As a general rule, licensing or other transfers of IP/technology entail less costs and difficulty than a joint venture, but also generate less financial return than actually "making" the product in the market (license agreements generally provide for a "royalty fee," which is often either a flat annual fee or a stated percentage of sales). A licensing agreement usually enables a firm to enter a foreign market quickly, and poses fewer financial and legal risks than owning and operating a foreign manufacturing facility or participating in an overseas joint venture. This is because licensing rarely requires significant levels of capital investment and does not require that the parties work closely together or demand continuous attention. Licensing also permits U.S. firms to overcome many of the tariff and nontariff barriers that frequently hamper the export of U.S. manufactured products.

There are also various drawbacks to a license in addition to the reduced profits. For instance, the licensor has reduced control over the product quality, distribution and marketing policies. The licensor will also have less control over the essential support services personnel employed for the purpose of manufacturing/selling the product or technology. Furthermore, if consideration is based on sales volume, the licensor must rely on the honesty of the licensee to report units sold.

Joint Venture: Joint ventures often involve additional costs and expense, but allow for both greater control and greater potential profits. As noted above, the income on a license agreement is usually limited in some way (a royalty based on a percentage of sales, etc). This is not the case for a joint venture, although the parties may agree to split any profits however they see fit. In addition, an international joint venture enables a firm to actually establish a marketing or manufacturing presence abroad with the assistance of a local foreign partner (whereas as licensor would generally have a much more limited presence in the new territory). The local partner may also provide added value through their knowledge of government workings, regulations, internal markets and distribution know-how. This knowledge may be particularly valuable in an unfamiliar or volatile region.

Additionally, a number of potential disadvantages are associated with a joint venture. A joint venture will likely require a greater investment than a license agreement (in both time and resources). Moreover, when compared to a license, there are additional risks inherent to a joint venture as they require significant levels ongoing cooperation between the parties and a greater presence in the foreign country. For example, if a disagreement or dispute between the parties results in reduced operational control, the U.S. company may experience reduced profits, increased operating costs, inferior product quality, exposure to product liability, and environmental litigation and fines. U.S. firms that wish to retain effective managerial control will find this issue important in negotiations with the prospective joint venture partner.

Thus, a choice between a license and joint venture will often turn on issues such as a potential market entrant's level of risk aversion and expectations regarding inter-entity cooperation, up-front investment costs, and profit margins.

Selecting a Partner

Regardless of whether a license agreement or a joint venture is selected as the appropriate vehicle, it is generally necessary to "partner" with another entity, although the level of cooperation varies depending on the specific type of market entry strategy and the scope of operations. Thus, selection of an appropriate "partner" is important, whether they are a licensee, partner, investor, etc. Selection of a partner is especially important with regards to considerations of quality control and regulatory compliance, both critical needs that will be fulfilled at the foreign location.

Deficiencies in any of the areas identified below would suggest that a potential "partner" must be examined with extraordinary care:

• Are the market entrant and the potential partner "culturally compatible" (both in terms of corporate culture and foreign social culture)?

• How does the potential partner, and its business operations, fit within the market entrant's overall strategic plan?

• What is the reputation of the potential partner within the foreign market generally and the specific industry (i.e., among customers, suppliers, regulators, and/or consumers)?

• What is the potential partner's organizational (i.e., management) level of skill and sophistication? What support financially and logistically will the potential partner require?

• What are the financial resources of the potential partner? Do they have sufficient access to capital? Is there any danger of insolvency?

• What financial reporting standards are applicable to the potential partner? Are third parties available to confirm compliance?

• With respect to IP, does the potential partner have sufficient technical and operational skill?

• If applicable, what is the potential partner's prior history with respect to the use or licensing of IP? Has it been involved in any previous litigations which involved claims of misappropriation of IP?

• Does the potential partner have sufficient manufacturing, distribution, and logistical experience?

• What is the potential partner's sales/marketing experience and capabilities?

• What is the potential partner's regulatory compliance capabilities and history?

• Technology Transfer

• The final issue to be considered are questions regarding technology (IP) transfer. As IP laws can differ based on the jurisdiction, entry into a foreign market may pose various risks related to an entrant's IP rights. Consequently, whether a license or joint venture is used to enter a foreign market, it is critically important to protect (i.e., prevent the exploitation of) any IP rights licensed or contributed to a joint venture vehicle.

• A potential market entrant should carefully consider each of the following questions in order to best protect its IP / trade secrets and maximize its return on investment:

• (a) If technology (as opposed to trademarks or names) is to be transferred:

• (i) Is the IP patented in the U.S.? Has the IP been patented in the new market? If not, when will this be possible?

• (ii) How will know-how or trade secrets be protected? It is important to be very careful when considering how the applicable law and other issues in the foreign jurisdiction will impact the protection of specific forms of IP. Poor choices can put key assets at risk.

• (iii) Pricing the transfer. Will a royalty be used or some other approach? Will the royalty be based on a flat fee or a percentage of sales? Will there be a minimum royalty?

• (b) If trademark/name/etc. is to be licensed:

• (i) Have appropriate filings been made in both the U.S. and the foreign jurisdiction? If not, when?

• (ii) Is prior use a requirement for registration in the foreign jurisdiction?

• (c) Is the involvement of key personnel required to complete the transfer? Can they be spared? May their knowledge be legally transferred?

• (d) Despite the legal arrangements, should key aspects of technology or know how remain under trade secret protection?

• (e) May the technology be legally exported/imported?

This article has reviewed various strategies and considerations relevant to operating in a foreign jurisdiction. Not only is it critically important that a business carefully select new markets, but equally important is selecting the proper market entry vehicle (and the selection of a related "partner," if applicable). We have experience advising clients on matters related to direct market entry, licensing agreements, joint ventures and technology transfer, and would welcome the opportunity to discuss any of these matters further.

Contract Risk Management - Looking Beyond the Words On the Page

By: Kimberly J. Decker, Esquire

Businesses enter into contracts every day as they purchase supplies, sell products and make business deals. Contracts are desirable because they describe the deal that was made and what each party to the contract is required to do. This helps to avoid problems and misunderstandings later. A good contract, however, also describes what happens if the deal goes bad - something you don't want to be caught negotiating after the fact.

If you do not have a form of sales and purchase terms and conditions that have been reviewed by legal counsel, or you do not understand how to use them to your best advantage, this should be your number one contract priority. Cutting and pasting provisions that you think look good from various contracts that you have worked on is **not** a good idea - you will likely end up with legal problems that far exceed the cost of hiring an attorney to do this work in the first place. A little work with a lawyer can help you manage your risks at a relatively low cost by customizing your contracts to address your particular business' risks. However, the legal words are only a portion of managing contract risks.

Managing Contract Risks

Below are the top five reasons why your contracts don't adequately manage your risks:

1. Your sales force does not use your standard forms. Having a standard contract is great, but you have to use it. Starting from your own form almost always gives you an edge, regardless of how much it is negotiated. However, depending on your industry and your bargaining power, there may be times where you have to start from someone else's contract form. When that happens, you should have someone on staff with a lot of contracting experience, or access to a lawyer. Contracts are rarely written in "plain English", and there are plenty of traps for the inexperienced negotiator.

2. Your sales force uses your standard forms, but they readily give away the "legal farm" to make deals happen. This approach will likely create a big headache - and unexpected liability - down the road. We recommend that you provide your sales force with at least basic training on contracts, the meaning of frequently used legal terms and why they are important. However, negotiators also need to also understand where they do - and don't - have authority to bargain. To provide that kind of guidance, we recommend that you identify, as a matter of business policy, what contract terms are:

- Absolutely critical to your business, and non-negotiable
- Important, but you might be willing to negotiate if necessary
- Routine and free to be negotiated

Making these decisions requires both business and legal input. Having this framework in place provides guidance to your sales force, gives consistency to your contractual relationships (almost everyone gets the same deal) and makes your sales force accountable not only for the business deal that they make, but for the legal concessions they may make.

3. Your sales people start from the wrong contract. This typically happens when someone sends out the contract from the last deal they did, which was negotiated, rather than your standard form. Ultimately, if the process of starting from the last deal continues, your contracts will end up offering less and less protection over time - usually, with no one the wiser until it is too late.

4. Contract attachments (often product specifications, pricing formulas and charts, project preparation duties, descriptions of services to be provided and the like) never get attached to the contract or, worse yet, no one can find the final, signed contract. This is often discovered when you already have a problem with the other

party, making that situation even more difficult to resolve. Assigning a department or person to manage your contracts and keep track of these details is vital.

5. You have risk-mitigating contract management policies and procedures in place that should keep the above issues from happening, but you don't really enforce them. As a result, over time, your sales people become more and more lax about these policies and end up reverting to their own way of handling negotiations and keeping track of contracts. We recommend that you provide a designated person or department to make decisions about when, and under what terms, you will negotiate contract terms. This person will help with those negotiations so you are only giving up what you have to in order to get the deal done. The designated person or department should also keep track of contracts, ensure that they are signed, have all exhibits and know when to pursue legal advice.

It is up to every business to decide what resources it is willing and able to devote to contract management. Contract management and its goals need to be supported from the top of the organization in order to be effective. Without the right corporate policies (and support of those policies), your sales people have no incentive to use your form contracts, to negotiate the best legal protection they can or to consult with legal counsel when necessary.

Ultimately, contract administration is just as vital to your business and risk management as the words of the contracts themselves. Good contract administration can ensure that you get the protection you expect from your legal forms, maintain consistency in the way you do business on the legal side, avoid future conflicts with business partners, help your organization keep track of contract expirations and deadlines and show business partners that you are organized and capable right from the start of the relationship.

Compliance Issues Inherent in Bring-Your-Own-Device Programs

By: Joshua L. Schwartz, Esquire

Employees use their own smartphones and tablets to perform a variety of work-related tasks. Even in companies that do not explicitly condone the use of personal devices for work use, employees often connect their devices to work systems. This increased use of personal devices in the workplace has brought with it a host of legal issues. Devices containing corporate or personal data can be lost or stolen. Viruses can infect corporate systems. Employees can use their devices to violate policies or company contracts. As a result, many companies have instituted formal bring-your-own-device (BYOD) programs to set expectations and ground rules for use of these devices. While there is no specific "best practice" when it comes to setting rules, this article will provide some basic considerations and strategies.

Security

The biggest risk to companies from BYOD is a potential breach of security. When a device is lost or hacked, not only is the company's own sensitive information at risk, but the loss may also breach confidentiality obligations that the company owes to third parties. Employers may choose to implement mobile device management (MDM) tools to manage risk in this area, including mandatory registration of employee devices, mandatory use of password protection, encryption for data sent through the corporate network, and remote wiping in the event a device is lost. Depending on the sophistication of an IT department, this may also limit the number of supported devices, and employees should obviously be made aware of such limits before purchasing any device.

An effective BYOD policy should also contain clear instructions on what activities are permitted on devices that have access to corporate information systems. Keep in mind that tools such as Siri or other standard smartphone applications retain instructions and information in the cloud for up to two years even if employees are not intentionally backing up to a cloud-based service. In addition, employees may be required to give their passwords over to an Apple store technician or even leave their devices overnight on some occasions. Employers, therefore, may want to take precautions to prevent sensitive information-especially information protected by HIPAA, financial regulations, or other state or federal law-from being downloaded into a device in the first place, or at least ensure that it is walled off from other information. Employers may also set rules limiting access of certain websites, backing up work-related information to cloud-based private services, letting friends or family use work devices, or connecting to work through unsecured wireless networks.

Consent

Consent is a key component to any BYOD program. Employees should understand that employers have the right to access, review, and delete data on their personal devices and that they have no expectation of privacy if they choose to use their devices for work purposes. At the same time, there are limits to what employers can monitor. Federal and state laws prohibit unauthorized access to certain electronically-stored information, including Social Security or driver's license numbers, and other personally identifiable information. Employers must also never install anything on an employee's personal device without first obtaining consent. All notices and requests for consent should be clearly written and should cover all potential needs an employer might have to access data on the device.

Litigation and Discovery

One of the reasons employers may need to gain access to personal devices is to comply with court orders or discovery requests. Organizations cannot object to producing information stored on personal devices on the basis that they have become comingled with an employee's personal information. To the extent possible, employers should adopt procedures to separate work and personal data at the outset, ensuring that work data (and only work data) is periodically backed up.

Other Legal Compliance Issues

This article will not address each and every challenge that might arise from a BYOD program. Nonetheless, beyond the right-of-access issues described above, any BYOD policy should include provisions addressing the following issues:

• Consider the tax consequences of reimbursements for devices, and make sure employees are aware of these consequences.

• Consider who will be responsible for lost or stolen devices and who will be responsible for malware or virus attacks associated with an employee's device. Relatedly, consider what kind of IT support the company will provide to personal devices in the event of malfunction.

• Make clear that policies concerning harassment and discrimination apply equally to conduct over mobile devices.

• Prohibit nonexempt employees from performing work "off the clock." Keep in mind that any work conducted on a personal device counts as "hours worked" for purposes of the Fair Labor Standards Act.

• Review the scope of software licenses before permitting employees to access the software from their personal devices. Some licenses limit access and use to devices owned by the company. By the same token, ensure that employees are not inappropriately using third-party software they download on their own for business use if only noncommercial use is permitted.

• Prepare for an employee's departure from the company. If an employee's device contains sensitive information, obtain advance consent to wipe this information before discharge. Of course, if the employees' device is subject to a legal hold as part of ongoing litigation, preserve any necessary information before wiping the device.

BYOD programs create significant risks for companies and require investment in technology to mitigate those risks. Failure to create clear policies regarding use of personal devices, however, can lead to even bigger risks. Once you have determined the contours of your BYOD plan, we can work with you to draft clear policies and procedures for a successful and efficient program.

Back To Top