1) INTRODUCTION TO TRADE SECRETS

A **trade secret** is a formula, practice, process, design, instrument, pattern, commercial method, or compilation of information which is not generally known or reasonably ascertainable by others, and by which a business can obtain an economic advantage over competitors or customers.[1] In some jurisdictions, such secrets are referred to as "confidential information", but are generally not referred to as "classified information" in the United States, since that refers to government secrets protected by a different set of laws and practices.

Definition

The precise language by which a trade secret is defined varies by jurisdiction (as do the particular types of information that are subject to trade secret protection). However, there are three factors that, although subject to differing interpretations, are common to all such definitions: a trade secret is information that:

- Is not generally known to the public;
- Confers some sort of economic benefit on its holder (where this benefit must derive *specifically* from its not being publicly known, not just from the value of the information itself);
- Is the subject of reasonable efforts to maintain its secrecy.

These three aspects are also incorporated in the TRIPS Agreement in Article 39.[2]

By comparison, under U.S. law, "A trade secret, as defined under 18 U.S.C. § 1839(3) (A), (B) (1996), has three parts: (1) information; (2) reasonable measures taken to protect the information; and (3) which derives independent economic value from not being publicly known".[3]

Broadly speaking, any confidential business information which provides an enterprise a competitive edge may be considered a trade secret. Trade secrets encompass manufacturing or industrial secrets and commercial secrets. The unauthorized use of such information by persons other than the holder is regarded as an unfair practice and a violation of the trade secret. Depending on the legal system, the protection of trade secrets forms part of the general concept of protection against unfair competition or is based on specific provisions or case law on the protection of confidential information.

The subject matter of trade secrets is usually defined in broad terms and includes sales methods, distribution methods, consumer profiles, advertising strategies, lists

of suppliers and clients, and manufacturing processes. While a final determination of what information constitutes a trade secret will depend on the circumstances of each individual case, clearly unfair practices in respect of secret information include industrial or commercial espionage, breach of contract and breach of confidence.

Protection of trade secrets

No registration procedures are involved for protection of a trade secret, and there is no specified time limit within which the secret may be protected. When a trade secret is leaked out, this breach of confidence is an action that may be taken in court, as this leak of the secret is unfair to the business/company, and may have harmful consequences.

However, not all information can be considered a trade secret. The court will consider the following when determining whether there has been a breach of confidence:

- The information was confidential to the business/company;
- The information has been revealed in breach of a promise of confidence; and/or
- The information was used in an improper way that has resulted in financial damage to the business/company.

HISTORY OF TRADE SECRETS

- "Trade Secret law is the oldest form of intellectual property protection, " according to Perritt. (Cave people?!)
- Back in Roman times, the law afforded relief against a person who induced another's employee (slave) to divulge secrets relating to the master's commercial affairs.
- Trade secrecy was practiced extensively in the European guilds in the Middle Ages and beyond.
- Modern law evolved in England in early 19th century — in response to the growing accumulation of technology and know-how and the increased mobility of employees.
- Recognized in U.S. by middle of 19th century, *Peabody v. Norfolk* (1868) held that a secret manufacturing process is property, protectable against misappropriation; secrecy obligation for an employee outlasts term of employment; a trade secret can be disclosed confidentially to others who need to practice it and a recipient can be enjoined from using a misappropriated trade secret.
- By the end of the 19th century the principal features of contemporary law were well established.
- 1939 the Restatement of Torts attempted to "codify" it.

6

Protecting Trade Secrets

Given today's progress in communication technologies and the speed at which information can be duplicated and moved, maintaining a trade secret is an everyday challenge. To meet this challenge an enterprise must consider the following:[3]

- Identify all valuable trade secrets and develop and put in place a trade secret protection policy and program;
- Educate employees about the importance of trade secrets and communicate to them the policy and the program;
- Carefully decide and review periodically as to which employees "need to know or use" the information and restrict access to trade secrets on a "need to know" or "need to use" basis;
- Apply physical and technological restrictions to access trade secrets;
- Limit and monitor public access to buildings that house trade secrets;
- Mark "secret" or "confidential" all documents containing trade secrets so as to avoid accidental or inadvertent disclosure;
- Sign confidentiality agreements with all relevant employees and also with outsiders who in one way or another may get access to an enterprise's trade secrets.

- Limit the number of people who can access such confidential information;
- Have employees sign non-disclosure agreements, which provide that they have to maintain confidential specific information that is disclosed to them;

Pros and Cons of Trade Secret Protection

When deciding whether to rely on trade secret protection, an enterprise must consider the advantages and disadvantages of doing so in comparison with other IP tools[2].

On the advantage side, a trade secret:

- Involves no registration costs
- Is not limited in time
- Is immediately effective
- Does not require disclosure or registration with the government

On the other hand, the disadvantages include:

- If the secret is embodied in a product, others may be able to discover the underlying secret and use it legally by "reverse engineering" it
- Protection is not granted if the secret is publicly disclosed
- Protection is only effective against improper acquisition and use or disclosure of the confidential information
- Protection is weaker than the protection granted to patents
- If the secret is embodied in a product, others may be able to discover the underlying secret and use it legally by “reverse engineering” it – see below
- A trade secret does not protect against those who independently come up with the same confidential idea. As a consequence, a trade secret that is also patentable may be patented by another if independently developed by that other. This is in contrast to patents that protect the owner of the patent even against those who happen to independently develop the same invention

The law does not punish fair discovery, which includes discovery by legal means like:

- Independent creation; trade secrets do not provide exclusivity, so anyone can discover your trade secret independently and use it or patent it.

2) Ten Ways To Maintain the Secrecy of Trade Secrets

One of the requirements for information to qualify as a trade secret is that the information must be "the subject of efforts that are reasonable under the circumstances to maintain its secrecy." Here are ten ways that employers can maintain the secrecy of trade secrets:

1. **Physical Protections:** Keep trade secrets in a locked room, cabinet, or vault. Employers can also use access rights (like key cards) to restrict who has physical access to the trade secret information, or they can maintain a log of individuals who had access to it and when.
2. **Digital Protections:** When trade secret information is stored digitally, user accounts and passwords can be used to control who has access to the information. If the information is transmitted via email or download, consider using encryption to prevent unauthorized disclosures.
3. **Label Information as "Confidential."** Although not absolutely necessary, including a label on any documents or information to make clear that it is "Confidential" is helpful.
4. **Destroy Old Documents or Data.** Trade secret information should not be placed in publicly accessible dumpsters or recycling bins in readable form. Instead, shred it before disposal. If trade secret information is stored on a computer or hard-drive, the computer or hard-drive should be wipe-cleaned or rendered inaccessible before disposal, too.
5. **Confidentiality Agreements:** Require employees who have access to trade secrets to sign confidentiality agreements. Confidentiality agreements should clearly define what information may not be disclosed and should authorize the employer to seek injunctive relief and damages in the result of a breach.
6. **Non-Disclosure Agreements:** For vendors or other third-parties who may have access to trade secrets, an employer can require the outside party to sign a non-disclosure agreement. Like a confidentiality agreement for employees, a non-disclosure agreement should clearly define what information is protected and authorize injunctive relief and damages in the event of a violation.
7. **Require Departing Employees To Return Company Property.** Employees who terminate their employment with the company should not be permitted to take company data with them. Instead, employment policies or agreements should clearly inform employees that all company data, whether in digital or hard-copy format, must be returned upon termination.
8. **Monitor Employee Emails or File Transfers**. Employees should not be permitted to email trade secret data to third-parties or personal email accounts or to copy trade secrets to external devices without authorization.

Periodically monitoring employee emails, either using software to detect key terms or via manual monitoring, is one way to detect unauthorized disclosures. Software is also available that can alert employers when files are copied to external devices.

9. **Don't Get a Patent.** Getting patent protection for an invention requires publicly disclosing how it works. If the protections of trade secret law are more valuable to a company than the limited monopoly provided by a patent, don't get a patent.
10. **Set a Good Example.** If employers want employees to protect the confidentiality of trade secrets, then the leaders and supervisors in the company should set a good example for the employees. If the leaders of the company are careless with trade secrets, the employees will likely be careless, too.

---

3) Physical security trade secrets

*By **Pamela Passman**, President and CEO, Center for Responsible Enterprise And Trade (CREATe.org), Washington DC, USA, and former Corporate Vice President and Deputy General Counsel, Global Corporate and Regulatory Affairs, Microsoft Corporation*

International cyberattacks with the intent to steal intellectual property (IP) continue to dominate the news, leaving many firms scrambling to shore up their computer networks to thwart such hacks.

However, the greatest threat may be already within a company. In more than 85 percent of the trade secret lawsuits in state and federal courts of the United States, the alleged misappropriator was either an employee or a business partner. That is the startling finding of A Statistical Analysis of Trade Secret Litigation in Federal Courts , which is believed to be the first statistical study on the subject.

How do you secure company trade secrets from both external threats and potential thieves already inside the company?

Increasingly, the courts are saying that firms need to take "reasonable steps" to protect confidential corporate assets, and these efforts include not only securing computer networks but also embedding trade secret protection into business operations and processes.

Determining the extent of "reasonable steps" can be challenging since governments have been vague about the term's definition. Laws and legislation also continue to evolve. However, research into court cases reveals the key elements of an effective trade secret protection plan. International cyber-attacks continue to attract media attention, but a recent study shows that the greatest threat may lie within companies

Protecting corporate crown jewels

The Statistical Analysis of Trade Secret Litigation in Federal Courts found that confidentiality agreements with employees and business partners were the most important factors when courts decided companies had taken reasonable measures to protect trade secrets. However, winning suits reveal that companies can and should take a number of additional steps to build a case for legal redress in the event that their corporate crown jewels are compromised.

The eight categories of a comprehensive protection plan include:

- creating agreements, policies, procedures and records to establish and document protection;
- establishing physical and electronic security and confidentiality measures;
- assessing risks to identify and prioritize trade secret vulnerabilities;
- establishing due diligence and ongoing third-party management procedures;
- instituting an information protection team;
- training and capacity building with employees and third parties;
- monitoring and measuring corporate efforts;
- taking corrective actions and continually improving policies and procedures.

1. Implement business procedures to augment non-disclosure agreements

As the study confirmed, confidentiality and non-disclosure agreements with employees and business partners constitute a great first line of defense and have won praise from the courts. In addition, the courts have said a company's overall corporate policy is important for maintaining confidentiality as evidence that it protects trade secrets.

2. Control physical and electronic access Most companies know that physical and electronic security is very important for protecting intellectual property, and courts are increasingly requiring it. For example, Japanese courts have found that a company must "implement physical and electronic access restrictions" in order for information to be deemed "kept secret" and thus protected by Japan's unfair competition rules for trade secrets.

3. Identify, assess and take steps to manage risks

It is difficult to make a case supporting trade secret theft without first identifying the information deemed to be confidential. As a first step, trade secrets should be documented in an internal registry. Next, an assessment of the risks should be made in the event that they are stolen. Which areas are most at risk of breaches and leaks? Which departments are most vulnerable? Once identified, companies should take

4. Create supply chain procedures and plans

Third parties, including those in joint ventures, suppliers, distributors and even customers, can have access to a company's trade secrets for manufacturing, product development or other collaborations. As these partners are a potential source of misappropriation, it is vital to have processes in place to protect confidential assets.

5. Conduct employee and vendor training

Training is essential for employees and third parties so both groups know what is expected of them when handling such information

6. Assemble a trade secret SWAT team

Problems arise when no one within a company has overall responsibility for protecting trade secrets and other confidential information. Courts have not looked favorably on companies that have not put a person or group in charge of trade secret protection. Best practices also point to establishing a cross-functional team with representation from those who can ensure that trade secret protection policies are being followed.

7. Make continual improvements

Unfortunately, trade secret protection might only be addressed at key milestones such as a new joint venture. In reality, such protections should be ongoing. Efforts to protect trade secrets should be monitored annually and procedures updated often to maintain consistency and ensure compliance.

8. Make trade secret protection a priority

Today, cyber threats, the digitization of information, complex supply chains and movement of employees between companies and continents put a company's valuable trade secrets at increased risk.

To protect critical business information, companies need to boost security and, importantly, put systems in place to ensure trade secret protection. This approach helps companies both mitigate risks and also meet the "reasonable steps" requirement in the event that trade secrets are compromised. Not doing so can risk a company's revenues, reputation and competitive edge.

4) **Employee access limitations**

Protecting Trade Secrets When Employees Departure form organaisation

According to a recent survey conducted by the Ponemon Institute (a research group in Arizona), 59 percent of departing employees steal confidential information from their employers. The survey, of nearly 1,000 persons who were laid off, fired or changed jobs in 2008, found: 53 percent of respondents download ed information onto a CD or DVD, 42 percent downloaded information onto a USB drive and 38 percent sent attachments to a personal e-mail account. Further, 82 percent of the respondents said their employers did not conduct a review of
their paper or electro nic documents in conjunction with their departure. While there is no sure-fire way to prevent employees from taking data when departing, there are a number of practical steps that employers can take to reduce the likelihood
that an employee will do so. By implementing these tips, an employer will also create a company culture where confidential information and trade secrets are taken seriously.
And, in the event that an employee steals information despite implementing these tips, the company will have positioned itself to demonstrate that it took all reasonable steps to prevent the misappropriation, thus increasing its odds of prevailing if it decides to
pursue litigation against the former employee. Establish a Confidentiality/Nondisclosure Policy Every employer should have a confidentiality policy prohibiting employees from disclosing or improperly using the company's confidential and trade secret information.In general terms, a confidentiality/nondisclosure policy should: (1) identify the company's information that is considered confidential and trade secret (in a way that is
meaningful and specific to the company's business); (2) prohibit unauthorized use or disclosure of the information; (3) set forth the consequences to the employee of

and (4) require the return of all confidential and trade secret information at the end of the employee's employment.
A confidentiality policy can be part of an employee handbook, a separate policy, or a free-standing agreement. If it is a policy
or part of an employee handbook, the employee should be required to sign an acknowledgment indicating that the employee has
received and agrees to be bound by the policy.Establish Specific "Protective" Policies/Protocols A company should also consider implementing a specific set of policies/protocols for protecting trade secrets and confidential information. The policies should set forth the measures the company takes to protect trade secrets
and confidential information. The goal should be to ensure that **the measures** are reasonable and enforceable, sufficient to be an effective deterrent, and withstand
scrutiny in litigation.

There are several issues to consider in crafting protective policies, including: Limiting access to confidential information and tr
ade secrets. Employees should only have access to confidential information that is needed to perform their job duties.

Limits on Physical Access This might include storing confidential information in a secure location protected by
security measures (e.g., requiring electronic card keys, badges, and/or a check-in policy for visitors). An employer may also want to consider a "check out" system whereby
access to its most important trade secrets is tracked at all times.

Limits on Electronic Access There are a number of methods to limitelectronic access, including requiring passwords to access certain company databases or systems, requiring passwords to be changed periodically, restricting certain segments of a company's computer network to certain employees, and "pop-up" warnings reminding employees of their confidentiality obligations each time certain systems or databases are accessed.
Employers may also want to consider prohibiting employees from using personal e-mail accounts to access confidential informatio

Identification of Confidential Documents An employer should consider regularly using restrictive legends such as "Confidential" or "For Internal Use Only" on documents that it deems confidential.
If an employer does decide to use such designations, it is important to train employees to use this designation consistently and in an appropriate manner. At the same time, it is

important to not overuse the designation in order to avoid diluting its relevance.

Access by Independent Contractors and Third Parties Employers who provide temporary access to confidential or trade secret documents to independent contractors or outside consultants should consider a policy for ensuring that those individuals also agree to the company's confidentiality policies.
Securing Remote Access Employers who allow remote access by its employees should consider appropriate security measures to ensure that such remote access is not misused.

Document Retention Employers should also consider how confidential documents are to be disposed of (e.g., shredding as opposed to simply throwing such documents in the trash).

Electronic Monitoring of Employees Employers should also address electronic monitoring to ensure that employees
understand and acknowledge that the company has the right to review their e-mail, Internet access, and computer use to check for misappropriation.
Doing so will prevent an employee from claiming that evidence obtained against them was obtained in a manner that violated their reasonable expectation of privacy.

Conduct Training on These Policies/Protocols Once policies/protocols for protecting trade secrets and confidential information are established, the next critical step is ensuring that the individuals responsible for
enforcing these policies/protocols understand the policies and actually follow them.

Confidentiality Obligations
Employers should also periodically remind employees of their confidentiality obligations.

Conduct Exit Interviews An exit interview is a great opportunity to convey to a departing employee the
seriousness with which the company treats confidential information and the xpectations the company has of the employee going forward. An exit interview should include a review of the types of confidential information that cannot be taken.
If the employee has previously executed any agreements regarding treatment of confidential information, this is the time to remind the employee of those agreements

Sign an Affidavit/Certification Employers should also consider requiring their employees to sign an
affidavit/certification stating that the employee has returned all data/property to the Company, and has not provided any data to anyone except in the usual and ordinary course of duties.

Disable Access Once the employer is aware that an employee is leaving, steps should be put in place to
limit or eliminate that employee's access to the company's trade secrets and confidential information. This might include changing passwords, requiring the return of
laptop computers and handheld devices, and eliminating remote access.

---

5) Employee Confidentiality Agreement – How It Works

By David Waring on May 27, 2014 | Hiring and Managing, Legal | Comments (0)

An employee confidentiality agreement is similar to a non-disclosure agreement. The difference is that a confidentiality agreement is with employees and contractors, where a non-disclosure agreement is with other firms.

Before we dive into the details on this topic, we also suggest you check out LegalZoom, our recommended online legal service. Form a business, access legal forms, connect to a lawyer and more. Visit LegalZoom to learn more.

An Employee Confidentiality Agreement can Help Retain Secret Information:

- First, the simple act of signing the agreement may impress upon the person the importance of confidentiality and prevent him or her from revealing the business's information.
- Second, there are state laws that protect trade secrets, but to take advantage of these laws the business must be able to show that it attempted to keep their information secret.
- Finally, a confidentiality agreement provides a basis to sue a current or former employee if he or she discloses or utilizes information in violation of an agreement. A confidentiality policy will demonstrate, in court, that something was meant to be kept confidential.

An employee confidentiality agreement should include broad language that requires employees and other individuals to protect non-public information about the company, its customers, and its employees. It should also instruct them not to use this non-public information or disclose this information with others, except as required by their current position with the company.

However, just because information is not explicitly shared that does prevent the information from being used by former employees when making decisions in new positions with other firms. This is why a business may also consider having employees sign a non-compete agreement in addition to a confidentiality agreement.

In order for trade secrets to be protected under an employee confidentiality agreement, you have to be able to provide proof that they are both proprietary and non-public. This means that the information is not known to the world at large but only to a small, select group of people within the company. Also, it should be labeled or otherwise communicated that the information is confidential. For an employee confidentiality agreement to prove effective, it should provide for the following:

- **Confidentiality** – A confidentiality provision would prohibit an employee or someone associated with the business from using or disclosing any trade secrets he or she may have had access to in the course of employment or interaction with the business. In short, the person agrees, on pain of legal sanctions, to ensure the confidentiality of the business secrets entrusted to him or her.
- **Restriction** – This clause is generally used only in employee confidentiality agreements. However, some businesses use this clause in all their confidentiality agreements. This provision ensures that the person will not compete with the business after leaving the job or once the interaction with the business is over. For example, the agreement might require that the employee not start his or her own company or take a job with a competitor for a specified period after leaving the job.
- **Assignment** – Since the person may develop valuable data in the course of employment or interaction with the business, this provision ensures that the data belongs to the business. In short, it addresses the question of who owns the resulting trade secret.
- **Severability** – Because one or more provisions of a confidentiality agreement could run afoul of the law, it's a good idea to include a severability clause. This clause would uphold the remaining provisions in

the agreement if a court should strike down one or more provisions as illegal or contrary to public policy.

- **Acknowledgement** – To keep the person from later pleading ignorance and challenging the agreement, the agreement should include a clause that stipulates that the person understands and voluntarily consents to the agreement's provisions.

Make sure the employee confidentiality agreement complies with the personnel manual. For an employee confidentiality agreement to be most effective, the personnel manual should delineate company policy on proprietary information. The business must define what constitutes a secret if the agreement is to work. This definition can be accomplished by taking the following steps:

- Labeling proprietary information as "secret and confidential".
- Limiting access to the information to employees with a "need to know" basis.
- Periodically searching employee lockers, desks, and PC files for unauthorized storage of information.
- Placing notices about the company's policy at all photocopying machines, computers, and facsimile machines.
- Limiting access to sensitive, corporate information by unauthorized persons.
- Requiring outside consultants and temporary employees, who have access to sensitive proprietary data, to sign confidentiality agreements.
    - Including an acknowledgement in termination notices that reminds employees of their continued obligation to not misuse corporate trade secrets.

Although no effort to secure corporate secrets is foolproof, confidentiality agreements are a step in the right direction. They deter misuse of information and place competitors on notice that they run the risk of litigation if they use dishonest insiders to steal secrets.

If you are looking for an online legal service to help put together your confidentiality agreement we recommend LegalZoom. Find out why here.

WHAT ELEMENTS SHOULD BE INCLUDED IN A CONFIDENTIALITY OR DISCLOSURE AGREEMENT?

A sample confidentiality agreement is contained in Appendix I. In general the agreement should address the following elements,

a) Consideration

Contract law requires that the confider give consideration (some form of payment to the recipient or detriment to the confider) in order to form a valid confidentiality agreement. In the case of an employee, consideration will likely be the promises of the overall employment agreement. In other situations, consideration may be the terms of the contract or the right of the recipient to examine the confidential information, thus enabling the recipient to make an informed decision as to whether or not to enter into a contract or make a bid. The consideration of the confidentiality agreement should be stated clearly, so as to prevent a later agreement that there was a lack of consideration.

b) Confidential Information

Every confidentiality agreement should contain a definition of Aconfidential information@. If the definition is too broad, it could be found void for restraint of trade. Thus, the client should carefully assess what information it really would be harmful to disclose. All such information should be included in the definition of "confidential information", but care should be taken to ensure that the definition is not over broad.

The definition should specifically exclude: information which is in the public domain, information already known to the recipient, information already known in the trade, as well as information that subsequently becomes known in the trade, general skill and knowledge: and information subsequently disclosed by a third party without obligation of confidence.

c) Onus of Proof

A clause which shifts the onus of proof may be inserted so that the recipient has the burden of proving that information was not confidential.

d) Use

It is important to specify the uses to which the recipient may put the confidential information. This use is likely the consideration, or part of the consideration, given by the confider.

e) Permitted Disclosures

Many agreements strictly prohibit any disclosure of the confidential information. The parties may prefer to insert a clause allowing disclosure in certain circumstances (e.g. legal proceedings).

f) Clarifying What is Confidential

The recipient may desire a clause requiring that all confidential information be marked "confidential"

g) Protective Measures

A clause requiring the recipient to take reasonable measures to keep the information confidential should be included. This may include a list of the specific steps to be taken by the recipient.

h) Duration of the Obligation

Although a clause stating the time limit during which confidentiality must be maintained may be included, such a clause is not required. An obligation of confidence may terminate by an agreement for consideration; the express or implied consent of the confider; or expiration of the confidentiality of the information.

i) Boilerplate

As with any contract, the parties may wish to include some boilerplate provisions: severance of wholly or partially unenforceable provisions from the rest of the agreement; a limitation period shorter than the normal six year period; a statement of absence of duress and full understanding of the contents of the agreement; signature of a witness to the agreement.

j) Restraint of Trade

As previously mentioned, protection afforded by a confidentiality agreement should not be over broad. A confidentiality agreement is a form of restrictive covenant. All provisions must be considered to make sure that they will not be void as unreasonable restraints of trade.

6) unfair competition in trade secrets

The law is called (Trade secrets and unfair competition law of 2000), and shall be effective after thirty ays s of the date of its publication in the Official Gazette.
Unfair Competition
Article 2
A. Any competition contradictory to the honest practices in the commercial and industrial activities shal
l be deemed one of the unfair competition acts and particularly the following:

1. The activities that may by nature cause confusion with entity, products or commercial or industrial activit
ies of one of competitors.
2. Untrue assumptions in practicing trade, whereby causing deprivation of trust from one of the competitors' entity, products or industrial or commercial activities.
3. The data or assumptions which use in commerce may mislead public in respect to the product's nature, methods of manufacturing, properties, amounts, and availability for use.
4. Any practice that reduce the product reputation, cause confusion in respect to the product general shape or presentation, or misl
ead the public on declaring the product price or the method of counting thereof.

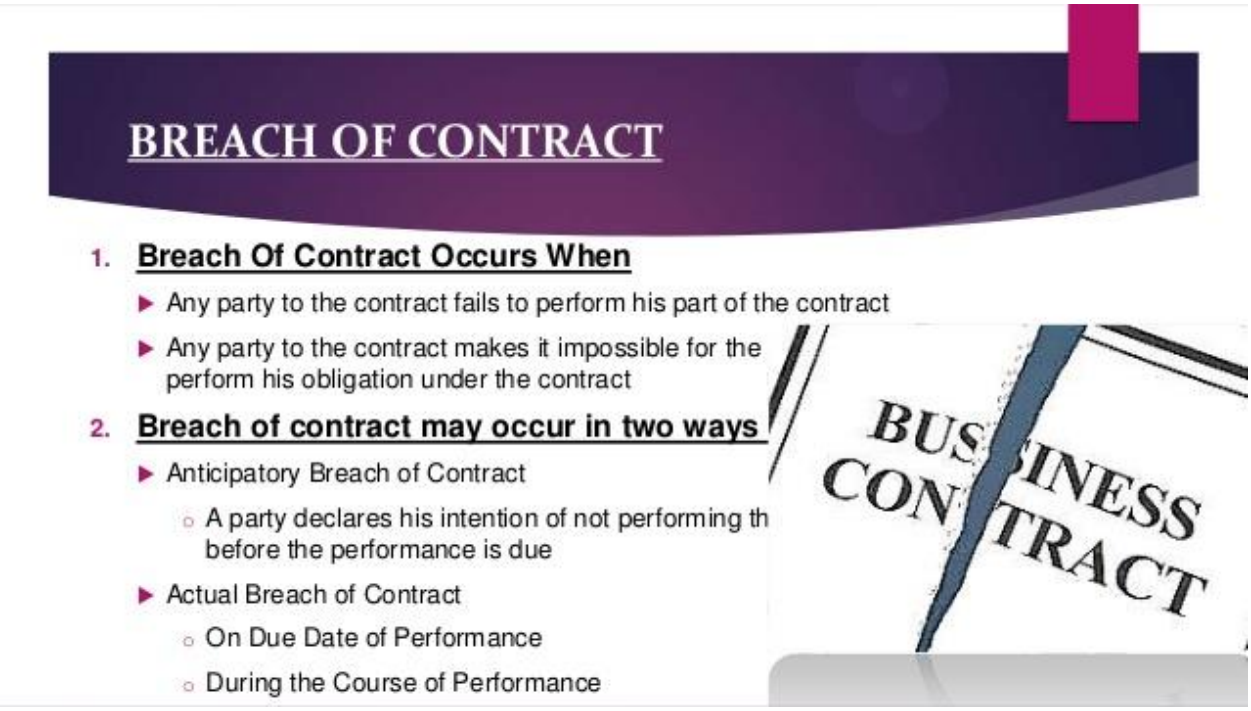
B. If the unfair competition relate to a trademark used in the kingdom either being registered or not and causes public misleading, provisions of paragraph (A) of such article shall be applied. C. The provisions of paragraphs (A) and (B
) of this article shall be applied on the services as necessary. Article 3 A. Any concerned party may claim ation for the damages caused to him as a
result of any unfair competition.
B. Upon filing a civil lawsuit related to unfair competition or during the examination of such lawsuit, any rested party may s
ubmit an application to the relevant court accompanied by bank or cash security accepted by the court for adopting the following measures:
1. Stopping such competition.
2. Precautionary Impoundment of the related articles and goods wherever it was.
3. Reserving the related evidences.
C.1. Any interested party may before filing his lawsuit, submit an application to the court accompanied by bank or cash security accepted by the court for adopting the measures provided in paragraph (B) of such article without further notifying the respondent. The court

shall approve for his request on proving any of the following:
– The competition has been committed against him.
– The competition is about to take place, and may cause great damage that is hard to be redressed.
– The interested party fears of loosing the competition evidence.
2. If the interested part did not file his lawsuit within eight days as of the date of the court approval, all the measures adopted for
this purpose shall be deemed void and null.
3. The respondent shall appeal against the court decision of adopting the precautionary measures before the court of appeal within eight days as of the date of his notification with the decision. The court decision shall be definite.
4. The respondent shall claim compensation for the harm caused to him, if proving that the plaintiff was not right in his request of adopting the precau
tionary measures or that the plaintiff did not file his lawsuit during the period provided in item (2) of such article.
D. The defendant shall claim compensation for the harm caused to him if the claim proved that the plaintiff wa
s not right in his claim.
E. The court shall in every case resort to the opinions of the experienced people.
F. The court shall decide to impound the goods subject of infringement and the materials and tools used mainly in the infringement. The court shall further decide to spoil or dispose of such products, materials
and goods in any commercial purpose.

Article 4
A. For the purposes of this law, any information are deemed trade secrets, if characterized by: 1. Is secret in the sense thatit is not generally known in its final form or its precise omponents, among or readily accessible to persons within the circles th
at normally deal with this kind of information in question. 2. Has commercial value because it is secret; and
3. Has been subject to reasonable steps under the circumstances, by the person lawfully
in control of the information, to keep it secret.
B. The provisions of such law shall not beapplied on trade secrets contradictory to general system or public morals.
Article 5
A. The person lawfully in control of the trade secret is every person having the right of its disclosure, sing and keeping.
B. The person lawfully in control of the secrets may prevent any person from misusing the protected trade secrets pursuant to such law.

Article 6
A. Any person obtaining, using or disclosing trade secrets in violation of the honest commercial practices, without the
consent of the person lawfully in control of such trade secrets, is deemed misuse of the trade secret.
B. For the purpose of applying provision of paragraph (A) of such article, the following shall be deemed iolation of
the honest commercial practices:
1. Breach of the contracts.
2. Breach and inducement to breach oftrusted secrecy of information.
3. The acquisition of trade secrets by third party who knows, or is able to know that such parties cquisition of such
secrets was a result of violating honest commercial practices. C. Individual access to trade secret or hrough reverse engi
neering shall not be deemed violation of the honest commercial practices. ----------
---

8) Breach of contract



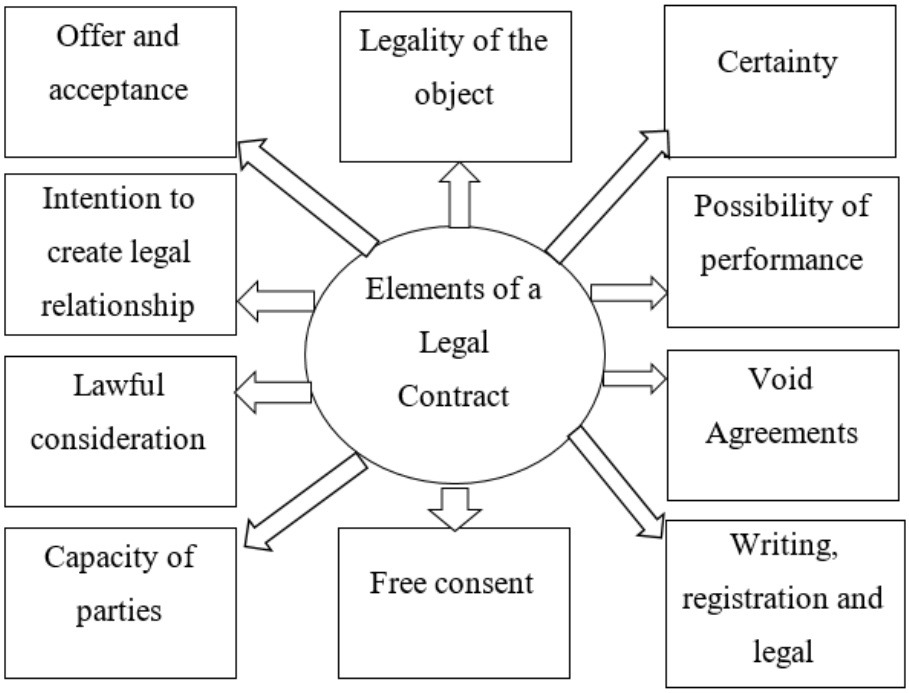


Fig: Elements of a legal contract

9) Applying State Law (or) Uniform Trade Secrets Act

1. Definitions

As used in this Act, unless the context requires otherwise:

(1) "Improper means" includes theft, bribery, misrepresentation, breach or inducement of a breach of duty to maintain secrecy, or espionage through electronic or other means.

(2) "Misappropriation " means: (i) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or (ii) disclosure or use of a trade secret of another without express or implied consent by a person who (A) used improper means to acquire knowledge of the trade secret; or (B) at the time of disclosure or use knew or had reason to know that his knowledge of the trade secret was (I) derived from or through a person who has utilized improper means to acquire it; (II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or (III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or (C) before a material change of his position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.

(3) "Person" means a natural person, corporation, business trust, estate, trust, partnership, association, joint venture, government, governmental subdivision or agency, or any other legal or commercial entity.

(4) "Trade secret" means information, including a formula, pattern, compilation, program device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

2. Injunctive Relief

(a) Actual or threatened misappropriation may be enjoined. Upon application to the court an injunction shall be terminated when the trade secret has ceased to exist, but the injunction may be continued for an additional reasonable period of time in order to eliminate commercial advantage that otherwise would be derived from the misappropriation.

(b) In exceptional circumstances, an injunction may condition future use upon payment of a reasonable royalty for no longer than the period of time for which use could have been prohibited. Exceptional circumstances include, but are not limited to, a material and prejudicial change of position prior to acquiring knowledge or reason to know of misappropriation that renders a prohibitive injunction inequitable.

(c) In appropriate circumstances, affirmative acts to protect a trade secret may be compelled by court order.

3. Damages

(a) Except to the extent that a material and prejudicial change of position prior to acquiring knowledge or reason to know of misappropriation renders a monetary recovery inequitable, a complainant is entitled to recover damages for misappropriation. Damages can include both the actual loss caused by misappropriation and the unjust enrichment caused by misappropriation that is not taken into account in computing actual loss. In lieu of damages measured by any other methods, the damages caused by misappropriation may be measured by imposition of liability for a reasonable royalty for a misappropriator's unauthorized disclosure or use of a trade secret.

(b) If willful and malicious misappropriation exists, the court may award exemplary damages in the amount not exceeding twice any award made under subsection (a).

4. Attorney's Fees

If (i) a claim of misappropriation is made in bad faith, (ii) a motion to terminate an injunction is made or resisted in bad faith, or (iii) willful and malicious misappropriation exists, the court may award reasonable attorney's fees to the prevailing party.

5. Preservation of Secrecy

In action under this Act, a court shall preserve the secrecy of an alleged trade secret by reasonable means, which may include granting protective orders in connection with discovery proceedings, holding in-camera hearings, sealing the records of the action, and ordering any person involved in the litigation not to disclose an alleged trade secret without prior court approval.

6. Statute of Limitations

An action for misappropriation must be brought within 3 years after the misappropriation is discovered or by the exercise of reasonable diligence should have been discovered. For the purposes of this section, a continuing misappropriation constitutes a single claim.

7. Effect on Other Law

(a) Except as provided in subsection (b), this [Act] displaces conflicting tort, restitutionary, and other law of this State providing civil remedies for misappropriation of a trade secret.

(b) This [Act] does not affect: (1) contractual remedies, whether or not based upon misappropriation of a trade secret; or (2) other civil remedies that are not based upon misappropriation of a trade secret; or (3) criminal remedies, whether or not based upon misappropriation of a trade secret.

8. Uniformity of Application and Construction

This act shall be applied and construed to effectuate its general purpose to make uniform the law with respect to the subject of this Act among states enacting it.

9. Short Title

This Act may be cited as the Uniform Trade Secrets Act.

10. Severability

If any provision of this Act or its application to any person or circumstances is held invalid, the invalidity does not affect other provisions or applications of the Act which can be given effect without the invalid provision or application, and to this end the provisions of this Act are severable. ----------