Protection of Employers’ Trade Secrets and Confidential Information

This Practice Note describes the legal protections and remedies available for employers in the area of trade secrets and confidential information. This Note provides a general overview of the law in this area. Specific state statutes and common law may impose additional or different requirements on employers, but the information contained in this resource will be useful and relevant to employers in every state.

Joseph W. Hammell and Jessie Collings, Dorsey & Whitney LLP

Protection of confidential corporate information is essential to a company’s capacity to develop products, provide services and gain economic advantages. Those who wrongfully acquire, misuse or disclose confidential company information can cause significant damage by impairing or destroying the value of the information. Employers may respond with legal action, but litigation remedies are often costly and inadequate and not all information is subject to equal protection. This Note highlights best practices for protecting trade secrets and other confidential information that may not rise to the level of trade secrets but nonetheless may be information the employer intends to protect. In particular, this Note addresses:

- The definition of a trade secret under both the Uniform Trade Secret Act (UTSA) and state common law.
- Examples of categories of information courts often protect as trade secrets.
- Legal recourse available to employers in the event of wrongful acquisition, misuse or disclosure of a trade secret by current or former employees.
- The importance of contracts and policies to protect trade secrets and other confidential information.
- Federal criminal sanctions and statutory remedies for trade secret theft.
- Characteristics of information that may be confidential, but not trade secret protected.
- Best practices to protect trade secrets and confidential information.

This Note primarily addresses trade secrets and confidential information in the context of the employer/employee relationship. However, many of the issues are relevant to trade secret and confidential information in the context of vendors, clients, independent contractors and other third parties.

OVERVIEW

Trade secrets and confidential information are both types of information that are kept secret and are valuable in part because they are not known by others. The key distinction between trade secrets and other sorts of confidential information is that trade secrets have greater legal protections. Information will only become a trade secret if it meets specific criteria established by either state statutory law or common law.
No broad federal statutory scheme exists to protect trade secrets, as exists for patents, trademarks and copyrights. Instead, trade secrets are primarily protected by state law, and to a limited extent by the federal Economic Espionage Act and Computer Fraud and Abuse Act (see Uniform Trade Secrets Act with 1985 Amendments).

Legal analysis of trade secrets is often fact-specific and state-specific, resulting in a substantial body of case law on the subject. Although there are distinctions in the law governing trade secrets from state to state, there are commonalities that all employers should understand to determine whether particular information is a trade secret and what can be done to protect it. For examples of information that may be protected as a trade secret, see below Judicially Recognized Examples of Trade Secrets.

Confidential information that does not rise to the level of a trade secret may still be protected, primarily through contractual rights and remedies. Employers should not assume that simply referring to information as a trade secret will entitle that information to trade secret protection.

TRADE SECRETS

DEFINITION UNDER THE UNIFORM TRADE SECRETS ACT

Although there is no single definition of a trade secret, most states have enacted a version (modified or unmodified) of the UTSA, which includes a definition of a trade secret. The UTSA is model legislation states can use to create their own state statute, and in most instances states have adopted the UTSA with little or no change.

The UTSA defines a trade secret as information, such as a formula, pattern, compilation, program device, method, technique or process that is both:

- **Valuable because of secrecy.** It is or potentially could be economically valuable at least in part because it is not known by others, or able to be discerned by others, who otherwise could benefit economically from using or disclosing it.
- **Protected by efforts to maintain secrecy.** It is protected by reasonable efforts to maintain its secrecy from others.

The model UTSA has been broadly incorporated into US law. The District of Columbia, the US Virgin Islands and all states except Massachusetts, New Jersey, New York and Texas have adopted a version of the model.

Valuable Because of Secrecy

Trade secret protection is extended to information that is secret and that has economic value because of its status as a secret. To help keep information secret, knowledge of trade secrets should be confined to those who “need to know.” Anyone with access to trade secret information (employees, as well as contractors, vendors and business partners) should be prohibited from disclosing the information to others. Ideally, employers impose this requirement by contract.

Outdated

If the information is no longer valuable, courts are unlikely to recognize the information as a trade secret. Information that is outdated by subsequent business developments may be a secret, but since it derives no independent economic value from being maintained as a secret, it cannot be a trade secret.

Protected by Efforts to Maintain Secrecy

To qualify as a trade secret, the party seeking trade secret protection must have made reasonable efforts to maintain the information’s secrecy. Courts assessing whether a company took reasonable measures to protect secrecy are likely to consider procedures and policies created to protect the information from outsider access and employee wrongful acquisition, misuse or disclosure. For tips on preservation of secrecy, see below Best Practices.

DEFINITION UNDER COMMON LAW

In states that have not adopted the UTSA or another statutory scheme to protect trade secrets, the definition and protections for trade secrets are determined by common law. Even in states where trade secrets have been defined by statute, prior judicial decisions and interpretations are important in adjudicating trade secret claims.
Courts sometimes look to the Restatement of Torts as a source of trade secret common law. The Restatement defines trade secrets as information used in business that gives the business an opportunity to gain an advantage over competitors who are not aware of it or using it. Examples of information under the Restatement of Torts that may be trade secrets include:

- Chemical compounds.
- Customer lists.
- Manufacturing processes.
- Formulae.
- Patterns.

The Restatement (Third) of Unfair Competition is another resource courts sometimes use when adjudicating trade secret claims. It defines trade secrets as information that may be used in business that is valuable and confidential enough to give either an actual or possible economic benefit over others.

JUDICIALLY RECOGNIZED EXAMPLES OF TRADE SECRETS

Because state law generally determines whether information is a trade secret, and varies from jurisdiction to jurisdiction, it is difficult to create an exhaustive list of trade secret protected information. Courts can be inconsistent, and it is possible for a court in one state to recognize a trade secret a court in another state would not. To be a trade secret, information must meet the legal requirements within the applicable jurisdiction, therefore no information can be described as a universally protected trade secret. However, the following are examples of information that have been recognized as trade secrets in a variety of states:

- Marketing plans.
- Commercial drawings.
- Recipes (such as chocolate chip cookies and pizza dough).
- Agricultural practices.
- Sales data.
- Manufacturing processes.
- Chemical formulae (such as insecticides and inks).
- Detailed information about customers.

COMMON LITIGATION ISSUES

The trade secret status of some categories of information is commonly litigated. For example:

- Customer lists. These may be trade secrets if they are protected from disclosure, expensive to create, substantively detailed and not publicly available. Alternatively, customer lists are unlikely to be trade secrets if they are simple compilations using publicly available information. The more difficult and expensive the development of the customer list or the harder it is to recreate, the more likely a court will consider it to be a trade secret.
- Theoretical ideas. It is common for business owners, companies or employees to seek protection for ideas that have not been developed into a specific process or formula. Although a specific strategy, plan or product idea may be a trade secret, a purely conceptual idea that has not been tested or developed and in which no investment has yet been made is unlikely to be a trade secret.

CONFIDENTIAL INFORMATION

Employers seeking to protect confidential information that is not a trade secret should create contractual obligations with those that will be exposed to the information, including employees, vendors, clients and business partners. As a rule, non-contractual legal protection for confidential information that does not rise to the level of a trade secret is rare.

Once employers create contractual protections for confidential information, there is some similarity to the way those protections are interpreted compared to the interpretation of trade secret claims. For example, like a trade secret analysis, a court’s analysis of a contractual claim regarding confidential information may include an inquiry into the extent to which an employer safeguards the information, whether the definition of the information is narrowly tailored to include only the truly confidential information and the value of its secrecy.

Courts typically are more willing to enforce confidentiality and non-disclosure agreements than non-compete agreements, but as a general rule courts will only enforce these agreements to the extent necessary to protect a legitimate business interest, such as preservation of confidential information.

LEGAL RECOURSE FOR VIOLATIONS BY EMPLOYEES

Employers may not recognize the need to protect their trade secrets and confidential information until the security of the information has been compromised. If an employer has concerns about unauthorized acquisition, use or disclosure of trade secrets, it should familiarize itself with its litigation options. Those whose trade secrets have been misappropriated may be able to make one or more of the following legal claims:

- Misappropriation.
- Breach of contract.
- Tortious interference with contract.
- Breach of duty of loyalty and/or fiduciary duty.

MISAPPROPRIATION

The principal and most common claim available to a company in this area is a claim for misappropriation of trade secrets. Because trade secrets are protected by state law, this claim is made under the applicable state’s trade secret law. The model URTSA, on which many state statutes are based, defines misappropriation as either of the following:

- Acquisition of a trade secret by improper means, or with knowledge or reason to know that it was acquired improperly.
Disclosure or use of a trade secret without the owner’s consent.

Requirements and remedies for a misappropriation claim depend on state law. State law variations determine:

- The elements required to prove misappropriation.
- Whether and under what circumstances employers can make legal claims for misappropriation against not only employees and former employees, but also competing employers and individual agents of the competing employers.
- Defenses against a misappropriation action.
- The relevant statute of limitations.
- The kind of relief available to successful plaintiffs, including injunctive relief and damages.

In some instances it may be difficult to prove that a former employee has used a trade secret or confidential information. In those circumstances, employers sometimes can use a theory of “inevitable disclosure.” If the former employee’s duties at his new employer are sufficiently similar to the duties at the former employer, then the court may conclude that it is inevitable that the former employee would use or disclose this information and therefore grant relief to the former employer.

The UTSA’s definition of misappropriation of a trade secret does not necessarily require that the defendant use the trade secret. Plaintiffs who can prove acquisition, but not use, may have a cause of action if they can show that the defendant knew or had reason to know that the trade secret was obtained improperly. Generally, if a plaintiff can show that a trade secret has been acquired but not used or disclosed, it can obtain injunctive relief and attorneys’ fees. However, that plaintiff likely will be unable to prove lost profits, unjust enrichment or other monetary damages.

If a state has adopted the UTSA or some other trade secret statute, state law must be reviewed to determine whether the statute preempts any other common law claims.

**BREACH OF CONTRACT**

If an employer had the foresight to require its employees to sign agreements containing confidentiality and non-disclosure provisions and/or non-competition restrictions, then the employer likely will also have a claim for breach of contract against a former employee who uses or discloses trade secrets or confidential information. If the agreement has been thoughtfully drafted, including provisions for immediate injunctive relief, the breach of contract claim may be the most formidable claim the employer has.

**TORTIOUS INTERFERENCE WITH CONTRACT**

Common law acknowledges the value of contracts and authorizes a cause of action against those who wrongfully interfere with contracts. This claim is often referred to as tortious interference with contract. Companies may have contractual rights in their relationships with vendors, clients, customers or employees, and this cause of action provides companies with a way to respond to the wrongful actions of others that undermine those contractual rights and relationships. Tortious interference with contract claims indirectly protects trade secrets by limiting a party’s capacity to use employer information to destabilize a company’s beneficial relationships and contracts with others, especially customers.

**BREACH OF DUTY OF LOYALTY AND/OR FIDUCIARY DUTY**

Common law imposes a duty of loyalty on all employees in most states. Managers, officers and others in a special position of trust owe an even higher duty, a fiduciary duty, to their employers. These duties regulate employee behavior, mandating good faith and prohibiting actions inconsistent with the employer’s best interest.

Employees who use company information to benefit themselves or a competitor violate their duty of loyalty. Individuals with a fiduciary duty have an even greater duty to act in the employer’s best interest and may affirmatively be required to take action for the employer’s benefit. For instance, an employee with a fiduciary duty to his employer who discovers a new formula or way of conducting business may be required to disclose such information to the employer for its benefit. These common law rules do not strictly prohibit all competition; instead they prohibit actions in conflict with the employer’s interests, such as the use of company resources or information in support of competitive activities.

**RISKS OF LITIGATION**

Besides the ordinary costs and risk of litigation, companies considering legal action should also be aware that lawsuits lead to discovery, which may result in additional disclosure of trade secret information unless adequate measures are taken to safeguard against further disclosure. Even when a confidentiality protective order is used in litigation to limit who has access to information disclosed in litigation, there still may be disclosure or dissemination of the employer’s trade secret information beyond what the employer would like.

**CONTRACTUAL AND POLICY PROTECTIONS WITH EMPLOYEES**

**CONFIDENTIALITY AGREEMENTS AND CLAUSES**

Employers often use confidentiality agreements or clauses as a means to protect confidential information and trade secrets. Subject to limitations under some states’ laws, confidentiality obligations for employees may be created through standalone agreements or as part of an employment agreement. These agreements are
signed by employees and should be supported by some benefit (otherwise known as consideration) for the employee.

In creating confidentiality agreements, employers should:

- **Define the information.** Define the confidential information and trade secrets that the employer intends to protect. Employers must achieve a thoughtful balance between defining the protected information too narrowly or specifically versus an overly broad definition that might be perceived by a court as unrealistic and therefore undercut the agreement’s enforceability. Employers should review and update as necessary the definition of confidential information on a regular basis so that the agreement accurately reflects information the company wants to protect.

- **Define the obligations.** Define the employee’s or the third party’s obligations to keep information confidential. If there are circumstances under which information should be disclosed (for legitimate business purposes), the agreement should provide instructions about how, when and to whom disclosure of information is appropriate.

- **Define the means to preserve confidentiality.** Provide guidance about where and how confidential and trade secret information should be maintained.

- **Define the obligations after termination of the relationship.** Make clear in the agreement that all the confidentiality obligations survive the termination of employment or the third party contract.

- **Be supported by consideration.** With respect to consideration:
  - if possible, confidentiality agreements should be entered into at the beginning of the employment (or third party) relationship and should specify that the relationship itself provides consideration for the obligation; and
  - if the agreement is entered into after the beginning of the relationship, additional consideration may be required, depending on the law of the given jurisdiction, to enforce the agreement. In some states, continued employment is sufficient to support the agreement. In other states, continued employment is insufficient and additional consideration is required.

Some companies believe they are adequately protecting their trade secrets if they simply require their employees to sign confidentiality agreements. However, confidentiality agreements have limitations, such as:

- **Insufficiency.** Confidentiality agreements alone, without additional measures, may be insufficient to protect the secrecy of information.

- **Drafting flaws.** A confidentiality agreement is only as good as the quality of its drafting. For example, confidentiality agreements authorizing disclosure outside the company on a need-to-know basis without requiring execution of a third party confidentiality agreement may not demonstrate a reasonable effort to protect secrecy.

**COMPREHENSIVE CONFIDENTIALITY POLICY**

In addition to agreements, employers should include comprehensive confidentiality policies in their employee handbooks or maintain stand-alone policies. Although these policies typically do not have the force of contract obligations, they remind employees of their obligations and employer expectations. They may also be used in litigation to demonstrate employee knowledge of confidentiality obligations.

Like agreements, these policies should define:

- Information to be protected.
- Obligations imposed.
- Required means to preserve confidentiality.

In addition, confidentiality policies should provide detail about which groups of employees may access confidential information and the specific protocols for maintaining confidentiality (for example, requiring that employees accompany visitors at all times or prohibiting employees from removing confidential material from the workplace).

**NON-COMPETE AGREEMENTS**

A non-compete agreement provides enhanced protection to employers by creating barriers to competitive activity for departing employees, which deprives them of the ability to use the employer’s trade secrets and confidential information. Although non-compete agreements are advantageous for employers, virtually every state views these agreements with disfavor and limits how far an employer can go in restricting competition from former employees. Some states prohibit employment non-compete agreements entirely. Even in states where non-competes are permitted, employers must meet a high standard to have them enforced. Among other benchmarks, employers must be able to demonstrate that the competitive restrictions are reasonable in scope (for example, geographically and in duration) when balanced against an employee’s interest in engaging in a livelihood.

**NON-SOLICITATION AGREEMENTS**

A non-solicitation agreement indirectly protects trade secrets by limiting a former employee’s freedom to “raid” company resources, such as employees, clients, customers, vendors or business partners. It prohibits a former employee
from approaching others, in an attempt to hire, retain or create contractual relationships with them, for a designated period of time. Non-solicitation agreements prevent former employees from using confidential and trade secret information that is valuable to the employer. Non-solicitation agreements can be stand-alone agreements or included in a non-compete agreement.

FEDERAL STATUTORY PROVISIONS

The Economic Espionage Act of 1996 does not allow employers to bring a legal claim, but it does create criminal penalties under federal law for unlawful trade secret activity. It prohibits trade secret theft and foreign economic espionage (meaning trade secret violations to benefit a foreign government or entity sponsored by a foreign government). Available penalties for trade secret theft include a fine (up to $5 million for organizations, unspecified for others) and up to ten years in prison. Available penalties for foreign economic espionage include a fine (up to $10 million for organizations and up to $500,000 for others) and up to 15 years in prison. For more information on the Economic Espionage Act, see US Attorneys’ Bulletin: The Economic Espionage Act of 1996, available at justice.gov/criminal/cybercrime/usamay2001_6.htm.

Additional criminal statutes govern unlawful use of and access to computers and electronic information. One such statute is the federal Computer Fraud and Abuse Act of 1986. The statute creates criminal penalties for the unauthorized access of another’s computer. The Computer Fraud and Abuse Act creates a civil cause of action for anyone who suffers damage or loss as a result of a violation of the act. The statute authorizes injunctive relief as well as damages. The statute does not require that the data accessed is a trade secret, only that it be valuable to the owner.

BEST PRACTICES

Employers should take the following steps to protect confidential and trade secret information:

- **Limit disclosure to those who need to know.** Keep the disclosure of confidential information and trade secrets limited to a discrete group of individuals who need the information to perform their jobs or for other legitimate business functions. Remind employees at meetings or events where confidential information will be disclosed that the information is confidential and that they have a duty to maintain confidentiality.

- **Put in place appropriate security measures.** For example:
  - mark documents or materials as confidential or trade secret as needed. Be consistent in this practice. Do not mark materials that are not truly trade secrets or confidential, and do not fail to designate material the company wishes to protect;
  - keep sensitive information physically guarded, for example by maintaining single entry into the building, using security personnel, creating sign-in and sign-out procedures, installing security cameras, posting signs limiting general access to areas where sensitive information is stored and using electronic access controls;
  - place strict limits and rules against allowing employees to remove information from the employer’s premises;
  - develop procedures for employee use of company laptops off site;
  - password protect trade secret and confidential material that is stored electronically, and ensure that only authorized individuals with a need to know the information have access to these passwords;
  - set up sufficient firewalls, encryption, anti-hacker initiatives, anti-virus software and other technical protections;
  - disable USB ports or other portable devices or drives on company computers;
  - maintain non-electrically stored items in locked cabinets or other secure areas;
  - place strict limits and rules on sharing confidential documents with clients, vendors or other third parties; and
  - create rules for visitors, including requiring that they sign acknowledgments prohibiting disclosure of information viewed or accessed during a visit, preventing them from bringing recording devices (such as cameras, cell phones, PDAs and USB drives) into restricted areas and requiring that they be accompanied by employees while in locations where sensitive information might become known.

- **Put in place appropriate contractual protections.** For example:
  - use confidentiality agreements;
  - use confidentiality policies with employees, which remind employees of their duties to preserve confidentiality; and
  - use non-compete agreements where authorized by state law.

- **Train employees.** Train employees on the importance of confidentiality and define the universe of information that must be protected. As part of that training:
  - ask employees to sign documents acknowledging receipt and understanding of confidentiality policies and training (in addition to any confidentiality agreement); and

For more information on the Computer Fraud and Abuse Act of 1986 and related criminal penalties, search Website Hacking, Viruses and Attacks on our website.
• remind employees of their obligations with respect to taking confidential or trade secret information off of the premises and using company laptops remotely.

Put in place appropriate departing employee procedures. Adopt a departing employee procedure aimed at minimizing risk of misappropriation. For example:

• provide departing employees with copies of any confidentiality agreement they signed during their employment and the company’s policy on confidential information and trade secrets;

• remind departing employees of their continuing obligations to keep information confidential. Ask departing employees to sign an acknowledgement of their continuing obligations;

• arrange exit interviews to determine where the employee will be working subsequently and if the employee may be engaging in competitive activity in the future;

• shut-off the employee’s access to computer files immediately upon termination;

• review the departing employee’s computer activity, hard drives, e-mail, voicemail and other communication records for the period before the employee’s termination if there is a high risk of misappropriation;

• ensure that the departing employee surrenders all company documents, files and other material (including electronic documents) and signs an acknowledgement of having done so;

• ensure that the departing employee returns all company access cards, PDAs and other electronic devices; and

• change electronic passwords as needed.

Ensure that confidential information does not appear in promotional or other public material. Exclude any confidential information and trade secrets from publications, marketing materials, websites, social media, advertisements and interviews.

Adopt a plan for a prompt response to inadvertent disclosure of trade secrets. For example:

• work with information technology professionals to develop a protocol to limit the spread of disclosed information;

• update the protocol as the company’s technology changes;

• ensure that new hires are trained on this protocol;

• remind employees and third parties of the need to maintain confidentiality; and

• adopt a protocol for contacting the individuals to whom inadvertent disclosure was made to alert them of the error and ask them to return or destroy the information. Ask them to sign acknowledgements that they have done so, if appropriate.

AUTHORS

Joseph Hammell and Jessie Collings are based in the Minneapolis office of Dorsey & Whitney LLP. Both are members of the firm’s Labor and Employment Group. Joe is a Partner who represents management in a variety of fields including employment law, business torts, restrictive covenants, trade secrets and general commercial litigation. Jessie is an Associate who provides litigation and counseling support on employment matters, including trade secrets and restrictive covenants.

Joseph W. Hammell
Partner
DORSEY & WHITNEY LLP

Jessie Collings
Associate
DORSEY & WHITNEY LLP