VENABLE LLP

technology transactions & outsourcing alert

AUTHORS:

Armand Zottola
AJZottola@Venable.com
202.344.8546

Robert Parr
RFParr@Venable.com
202.344.4594

MAY 2013

Guidelines for Protecting Company Trade Secrets

"Trade secrets" are generally defined as confidential proprietary information that provides a business with a competitive advantage or actual or potential economic benefit. Trade secrets are protected under the Economic Espionage Act of 1994 (EEA) at the federal level, and 48 states have enacted statutes largely patterned upon the Uniform Trade Secrets Act[1] (UTSA) (collectively, "Statutes"). Under these Statutes, company information that may be protectable as a trade secret must specifically have three characteristics:

i. the information must fall within the defined "information" eligible for protection;

ii. such information must derive independent economic value from not being generally known or readily ascertainable by appropriate means by others; and

iii. the information must be the subject of reasonable efforts to maintain its secrecy.

Trade secret theft and economic espionage against U.S. companies continue to accelerate. Even a single trade secret security breach may substantially undermine a company's ability to compete in the marketplace. In recognition of this threat, Congress and certain state legislatures have recently passed some legislation that has broadened and strengthened trade secret protection. Consequently, it has become important for private sector businesses to ensure that they sufficiently safeguard all proprietary and customer information that may qualify as protectable trade secrets. To that end, this guide provides jurisdiction-neutral explanations of key trade secrets concepts, and offers pointers on how to identify and sufficiently protect potential trade secret information.

(1) Determine Which Data Constitutes "Information"

There is no bright-line definition as to what subject matter constitutes "information" under the Statutes. The aforementioned statutes generally define "information" broadly to include:

- All forms and types of financial, business, scientific, technical, economic, and engineering information;
- Patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, or codes;
- Information related to single or multiple events, negative data points that have commercial value such as the results of lengthy and expensive research which prove that a certain process will not work; and
- Information that can be held or stored in any medium (whether physically, photographically, graphically, electronically, or in writing).

[1] Some jurisdictions, such as Texas, California, Arkansas and Illinois, have adopted trade secret laws that depart substantially from the UTSA. Therefore, businesses should carefully research local trade secret laws in the relevant jurisdiction(s) in addition to following this guidance to ensure that they adequately identify and protect all potential trade secret information.

Courts have similarly interpreted "information" to cover virtually any knowledge, data or process used to conduct business that is protected from public disclosure. For example, the following categories of information have been found by courts of law to constitute trade secrets:

- Pricing techniques
- Marketing techniques
- The identity and requirements of customers
- Financial information
- Customer information
- Maintenance of data on customer lists and needs
- Sources of supplies
- Pricing data and figures
- Manufacturing processes
- Product compositions
- Expiration lists (often used in the insurance industry)
- Buy books
- Cost books
- Customer books or lists
- Confidential costs

As a result, businesses should realize that vast amounts of their data may constitute "information" eligible for trade secret protection.

2) "Economically Valuable" and "Not Readily Ascertainable" Information

Information must also retain "economic value" and not be "readily ascertainable" by others. Although determined subjectively at first by the claimant, courts of law determine whether information satisfies this standard on a case-by-case basis depending on the unique facts and circumstances of a proceeding. However, when determining value and whether information is readily ascertainable, courts of law generally consider the following factors:

- Reasonable protective measures (not all conceivable efforts) have been established to protect the information from both internal and external theft or misappropriation;
- The information is known by a limited number of employees or other parties (in a "confidential relationship" with the company) who possess a business-need-to-know;
- The information has actual or potential commercial value to a company or provides a company with a competitive advantage in the marketplace;
- The company devoted significant time, money and other resources to develop the information;
- The information would be useful to competitors and requires a significant investment of time, expense or effort to duplicate or acquire, even if some or all competitors possess the know-how and means to independently create their own versions of the information; and
- The information is not generally known to the public, or to other persons or businesses outside of the company who can obtain economic value from its disclosure.

The more of these factors that apply to particular company information, the greater the likelihood a court of law would ultimately conclude the information constitutes a trade secret.

3) Implement Reasonable Protective Measures to Ensure Secrecy

Information that retains economic value and is not readily ascertainable must also be subject to reasonable security measures. Businesses should implement reasonable technical, administrative, contractual and physical safeguards appropriately tailored to the day-to-day business of the particular enterprise, the confidential information sought to be protected, the community in which the company operates, and the established awareness of the individual participants to whom access to the information may be granted. Appropriate security measures should result from some consideration of the foregoing factors and an assessment of what safeguards are most compatible with the practicalities and efficiencies of the unique workplace.

A. WRITTEN INFORMATION SECURITY POLICIES

Companies should implement written information security and confidentiality programs that incorporate proven information security and confidentiality principles. These programs should be regularly and consistently enforced in order to satisfy the third element of the trade secrets test. Below is a list of some suggested measures that companies may adopt to protect confidential information that is eligible for trade secret status:

- *Risk identification and assessment*. Use commercially reasonable efforts to (i) identify and assess reasonably foreseeable threats to the security of confidential information; (ii) identify and assess the likelihood of harm and

potential damage flowing from such threats; and (iii) gauge the need to adjust security protocols to address new threats and program deficiencies.

- *Safeguards*. Implement certain administrative, technical and physical safeguards to prevent the unauthorized access to and use or disclosure of confidential information:
  - **Administrative Safeguards**
    - *Compartmentalize information*. Restrict access to confidential information on a business-need-to-know basis. These restrictions could include dividing information into pieces and precluding all but a few employees from having access to the entirety.
    - *Use unique employee identifiers*. Assign each employee with computer access a unique identification number to enable system tracking.
    - *Audit security protocols*. Regularly review the efficacy of security procedures to address new threats and program deficiencies.
    - *Legending materials*. Classify information according to type and sensitivity and mark documents with an appropriate legend (such as "confidential" or "top secret").
    - *Distribute employee manuals*. Circulate an employee handbook that (i) outlines what constitutes confidential information or a "trade secret"; (ii) explains the essential nature of the information security and confidentiality program; (iii) reproduces the material terms of any restrictive covenants; and (iv) describes company policies regarding social media use, remote access and mobile devices, and employee privacy.
    - *Conduct employee training*. Regularly train employees about information secrecy, and issue periodic reminders about secrecy obligations.
    - *Entrance interviews*. Conduct entrance interviews for new hires to determine whether they are subject to restrictive covenants with former employers or whether their new employment status raises a substantial likelihood that the company will improperly use a former employer's trade secrets.
    - *Exit interviews*. Conduct exit interviews with departing personnel to (i) review secrecy obligations and restrictive covenants; and (ii) require the departing employee to sign a statement providing that such employee has returned all company materials containing confidential information, and understands and agrees to abide by post-employment obligations.
    - *Review released content*. Review company advertising, websites, press releases, seminar content and articles before publication to ensure that trade secret information is not inadvertently disclosed.
    - *Consideration of response plan*. Consider implementing a trade secret breach plan that calls for (i) injunctive relief when the perpetrator is known and the trade secret has not yet been widely disseminated; or (ii) a general exclusion order from the U.S. International Trade Commission to bar the importation of goods resulting from unfair trade practices; or, in the extreme case and as a last resort, (iii) an application for patent protection.
  - Technical Safeguards
    - *Encrypt data*. Encrypt confidential information that is stored and transmitted across open, public networks.
    - *Technical restrictions*. Limit access to confidential information through passwords and network firewalls.
    - *Run antivirus software*. Use and regularly update antivirus software on all systems commonly affected by malware.
    - *Avoid default passwords*. Do not use vendor-supplied defaults for system passwords and other security parameters.
    - *Catalogue data access*. Track and monitor all access to network resources and confidential information.
    - *Monitor large downloads and emails*. Monitor sizeable downloads or emails with large attachments to help quickly detect potential theft of confidential information.
  - Physical Safeguards
    - *Guards*. Station security personnel at each facility entrance.

- *Signage*. Post warning or cautionary signs in areas near where confidential information is located.
- *Limit visitor access*. Provide limited visitor tours of company plants and facilities, if at all.
- *Surveillance*. Establish security and surveillance procedures to prevent any unpermitted entry into company facilities or removal of confidential information.
- *Physical barriers*. Lock up hardcopy materials and require key-card access to sensitive areas of company facilities.

B. CONTRACTUAL METHODS

Business relationships with parties that may involve disclosure or exposure to company information pose significant threats to the confidentiality of such information. Below is a list of suggested concepts that should be incorporated, as applicable, into businesses agreements with employees, licensees, service providers, contractors, subcontractors, consultants and prospective purchasers of all or part of a business (together, "Business Counterparties").

- *Confidentiality*. Establish permitted uses and disclosures of confidential information by Business Counterparties, and provide that such parties cannot use or further disclose confidential information except upon the written consent by the company or as permitted or required by the contract or law.
  - *Disclosure and assignment of inventions*. Consider coupling nondisclosure requirements with assignment of invention or work obligations. In particular, require employees to promptly and fully inform the company in writing of any inventions, discoveries, works, concepts and ideas ("Developments") created by the employee.
  - *Contractors*. Ensure that contractors are similarly required to inform the company of any Developments created during performance of their duties.
- *Terms of employment*. Require employees to execute written agreements that establish, among other things, clear policies regarding (i) the right to download confidential information onto external or mobile devices; (ii) the ownership and control of confidential information, including, without limitation, work-related social media accounts and confidential information saved on external or mobile devices; (iii) the return or destruction of information upon resignation; and (iv) the obligation to provide notice about subsequent places of employment and the employee's proposed activities or duties for the new employer.
- *Disclosure of restrictive covenants*. Require new employees to represent in writing that they are not currently bound by a covenant not to compete or a nonsolicitation clause with a prior employer.
- *Possession of another's confidential information*. Require new employees to represent in writing that they will not utilize or disclose any confidential information belonging to a prior employer during their tenure at the new company. Companies should also provide employees with the opportunity to decline assignment of rights to intellectual property created or developed under a prior employment relationship.
- *Return of confidential materials*. Require employees of the company and, in particular, new employees, to promise that upon termination, they will promptly deliver to the company all confidential materials.
- *Restrictive covenants*. Consider having employees sign nonsolicitation and/or noncompetition agreements that restrict a narrowly specified scope of activity for a reasonable period of time and within a reasonable geographic territory. The legal rules governing the enforceability of these clauses varies widely among the states. Therefore, carefully research statutes and case law on the enforceability of restrictive covenants in the relevant jurisdictions before implementation.
- *Third-party contracts*. Require contracts with Business Counterparties to contain, as applicable, and as tailored to the Business Counterparty, provisions that include the abovementioned concepts. Additionally, require Business Counterparties to ensure that any subcontractor they engage on their behalf agrees to the same restrictions and conditions that apply to the Business Counterparty with respect to confidential information.

If you have any questions about this alert, please contact one of the authors or a member of the **Technology Transactions & Outsourcing Practice Group**