Defend Trade Secret Act—Over one year later.
Will the Court grant you a preliminary injunction?

ABA Cyberspace Law Institute/Winter Working Meeting
January 26-27, 2018

Phong Nguyen, Partner, BakerHostetler, Washington, DC

It has been over a year since Defend Trade Secret Act (DTSA) has been implemented that allows for a misappropriation of a trade secret complained to be filed in Federal Court. Come and learn procedures that Courts look to in order to grant preliminary injunctions when a trade secret has been misappropriated. Being able to obtain an immediate preliminary injunction from the Courts can combat the spread of your client’s trade secrets.

Phong Nguyen closely collaborates with in-house counsel to develop robust strategies that best serve his clients' needs. He is proactive in managing patent portfolios to obtain varying scopes of protection and in strategically advising on the acquiring and divesting of patents. He prepares and prosecutes patent applications for clients in various technologies including computers, software (interfaces), cellular phones, wireless transmission, semiconductors, electronic diagnostic devices, oil tool equipment, medical devices (contact lenses with sensors) and mechanical devices, while litigating and participating in adversary proceedings related to their patents. He analyzes the markets and attends conventions in which his clients operate, and uses the knowledge he gains to develop valued-added portfolios and litigation strategies beneficial to business success. He renders opinions regarding infringement, freedom to operate and validity of patents. He also drafts and negotiates license agreements and conducts due diligence.
Defend Trade Secrets Act—One+ Year Later.
Will the Court grant you a preliminary injunction?

Phong Nguyen, Partner, BakerHostetler, Washington, DC

More than a year has passed since the enactment of the Defend Trade Secrets Act (DTSA) (18 U.S.C. § 1832, et seq.), which amended the Economic Espionage Act of 1996 (18 U.S.C. § 1831, et seq.) and created a new federal civil cause of action for misappropriation of trade secrets. However, the DTSA doesn’t preempt any misappropriation of trade secrets state law so thus, they can be filed in parallel. Remedies under the DTSA include (1) ex parte seizures; (2) temporary restraining orders (TRO); (3) money damages including reasonable royalties; and (4) attorney fees.

The DTSA provides uniform definitions for the critical terms “trade secret,” “misappropriation,” and “improper means.” Specifically, trade secret is defined as: “all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if (A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.”

Under the DTSA, misappropriation is defined as follows:

“(A) 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
“(B) disclosure or use of a trade secret of another without express or implied consent by a person who—
“(i) used improper means to acquire knowledge of the trade secret;
“(ii) at the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was—
“(I) derived from or through a person who had used improper means to acquire the trade secret;
“(II) acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret; or
“(III) derived from or through a person who owed a duty to the person seeking relief to maintain the secrecy of the trade secret or limit the use of the trade secret; or
“(iii) before a material change of the position of the person, knew or had reason to know that—
“(I) the trade secret was a trade secret; and
“(II) knowledge of the trade secret had been acquired by accident or mistake.
Under the DTSA, misappropriation is defined as follows:

“(6) the term ‘improper means’—
“(A) includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means; and
“(B) does not include reverse engineering, independent derivation, or any other lawful means of acquisition;

**Trade Secret Considerations**

What Are Your Different Potential Trade Secrets?

- Sales and marketing information
  - Business methods
  - Business plans
  - Business forecasts
  - Competitors analysis information
  - Sales-call reports
  - Customer, vendor, and distributor lists and databases
  - Customer needs, buying habits and preferences
  - Proprietary sales and marketing information
  - Commission structure

- Products and engineering information
  - R & D information
  - Product information
  - Production plans
  - Specifications for production processes and machinery
  - Pricing and costs information
  - Overhead information
  - Personnel information
  - Engineering plans
  - Bill of Materials
  - Know-how
  - Manuals
  - Computer programs
  - Computer data bases
  - Designs
  - Patterns
  - Blue prints
  - Maps
  - Formulas
  - Ingredients
  - Devices
➢ Machine processes
➢ Manufacturing techniques
➢ Quality control procedures, manuals or records
➢ Manufacturing methods
➢ Repair techniques
➢ Repair methods
➢ Processes
➢ Systems

• Financial information
  ➢ Proprietary financial information
  ➢ Internal financial documents
  ➢ Budgets and forecasts
  ➢ Product margins
  ➢ Product costs and pricing
  ➢ Operating reports
  ➢ Profit and loss (P&L) statements

• Internal administrative information
  ➢ Proprietary administrative information
  ➢ Internal organization chart
  ➢ Key personnel information (i.e., salary/compensation information)
  ➢ Strategic business plans
  ➢ Internal computer software
  ➢ Where proprietary information are stored

**Identify Location and Marking of Trade Secrets.**

• Marking the trade secret with markings (“Company Sensitive” or “Company Proprietary” or “Company Confidential”)

• Identify the medium in which the trade secrets are stored:
  ➢ Electronic (company-owned or employee-owned electronic devices or both)
  ➢ Computer (local and servers)
  ➢ Paper documents (filing cabinets, folders)
  ➢ Human memory
  ➢ CDs and other electronic media (Flash/Thumb drivers)

• Identify the locations at which the trade secrets are stored
  ➢ Company headquarters
  ➢ Satellite offices
  ➢ Work sites/Desks
  ➢ Offsite locations (clients, vendors, home, partners)

**What Procedures Are In Place To Restrict Access to Trade Secrets?**
• Security procedures
  ➢ Premises (name tags, receptionists, locks, key or FOB access, biometrics)
  ➢ Computer Network (spyware, virus protection, cybersecurity, encryption)
  ➢ Backup of computer network to a secured server
  ➢ Access/Authorization (user name and password, biometrics, two-factor)
  ➢ Counter-Espionage (security checks, penetration checks)
  ➢ Segregate trade secrets from other Company information
  ➢ Assign a specific employee the responsibility for managing the confidential information
  ➢ Transmit trade secrets only through secure means (encryption, passwords, secure sites)
  ➢ Develop an appropriate policy for destruction of trade secrets stored in various means
  ➢ Install software that warns employees when they access trade secrets, notifies the company when trade secrets are accessed, and allows the company to remotely monitor or wipe trade secrets on company-owned portable electronic devices (when employees consent)

• Are company confidentiality policies reviewed and updated on a regular basis?

• Are regular audits conducted of company policies and procedures used to protect confidential information and are they updated and revised as needed?

• Are confidentiality/non-disclosure provisions in all agreements and policies including Notice of the immunity provisions?

• Are procedures in place for correcting inadvertent disclosure?

• Are policies and procedures in place for pursuing theft of trade secrets and other confidential information?

• Is there an appropriate document-retention and destruction policy?
Trade Secrets and Employee Relations Protocols

Candidate Considerations.

- The interviewer should take notes on a standard form identifying key points to be covered during the interview.

- Have a written job description that identifies the essential job functions of the position; identifies the interactions that the position will have with trade secrets, confidential information, and intangible assets; identifies the types of agreements that the employee must execute such as confidentiality agreements, trade secrets agreements, non-compete agreements, other restrictive covenants, disclosure and assignment of IP agreements.

- All candidates should complete a standard employment application form which requires that the candidate acknowledges that the company respects the trade secrets, confidential information, and intangible assets of third-parties, and that the company similarly protects its own; requires a candidate to disclose any prior enforceable agreements that would impact the candidate’s ability to perform the essential job functions of the position; affirm in writing that the candidate will abide by any such agreements and will not disclose any trade secrets or confidential information of any current or former employer as part of the application process or during employment; and affirm that the candidate has received Notice of the immunity provisions of the DTSA; and requires the candidate to identify in general terms the types of trade secrets and confidential information that the candidate holds.

- A candidate should receive a copy of the completed application.

- Candidates should sign and receive the signed copy a confidentiality/non-disclosure agreement if they will be exposed to any confidential information during the interviewing process and such agreement should provide Notice of the DTSA immunity provision or refer to a policy containing the DTSA Notice.

- Prior to accepting a position, a candidate should receive a copy of any confidentiality/non-disclosure agreements or restrictive covenants that he or she will be required to sign as a condition of employment.

- The company should design and use a standard protocol for interviewing applicants. The interviewer should take notes on a standard form identifying key points to be covered during the interview. The interviewer reiterates key points about confidential information, such as: The company respects and protects the trade secrets and confidential information of others.
The company protects its own trade secrets and confidential information.

The candidate should not disclose any trade secrets or confidential information of other during the interview process.

The company expects the candidate to abide by all agreements with any current or former employers.

The interviewer explains the types of agreements that the successful candidate will be expected to sign to protect the company’s trade secrets, confidential information, and intangible assets.

The interviewer explains when disclosures of trade secrets is prohibited and when such disclosures will not incur liability under any state and federal trade secret laws pursuant to the Immunity provisions of the DTSA.

Before a candidate is asked to return for a second interview, the company should receive and review copies of all agreements that the candidate has signed with current or former employers.

The company human resources department should maintain all applications, resumes, agreements, and interview notes in individual files for each candidate.

Extending A Job Offer.

A candidate should receive copies of all agreements that he or she will be expected to sign if he or she accepts the job and is encouraged to review the agreements with counsel and with family members before signing them.

The candidate should receive a copy of the company’s employee handbook and confidentiality policies that should include a Notice of the Immunity Provisions of the DTSA.

The interviewer should instruct the candidate to remain loyal to the current employer and caution the candidate

  ___to refrain from removing original records from that employer;
  ___to work with employer to return coordinate the return of all confidential information; but
  ___not to advise clients of departure prior to resignation;
  ___not to advise coworkers of departure prior to resignation;
  ___not to solicit customers;
  ___not to solicit coworkers to leave that employer.
Employee Relations.

- As part of an annual employee evaluation, review the company policies on trade secrets, confidential information, electronic services and communicates, among other policies and procedures, with each employee. Have each employee sign an acknowledgement that the person conducting the evaluation meeting reviewed the policies.

- Protect confidential information from employees’ access from remote locations.

- Restrict access to sensitive information on a need-to-know basis.

- Incorporate appropriate training and agreements with those who have a “need to know.”

Create A Culture Of Confidentiality In The Work Place.

- Regularly discuss the obligations of confidentiality in employee meetings.

- Review obligations of confidentiality as part of employees’ annual review.

- Document independent development of trade secrets and other confidential information.

- Keep confidential information off of the company’s website and make sure it is not in other marketing materials. Avoid disclosing confidential information through electronic communications.

- Implement policies regarding use and disclosure of trade secret/confidential information through social media (Facebook, LinkedIn and Twitter).

- Follow the company’s policy on confidentiality.

Employee Departures.

- Determine the type of information the company is most concerned about losing with the departure of the employee.

- Inventory sensitive documents to which the employee has had access.

- Inventory any electronic materials to which the employee has had access, including software source code. Note the “last edit” dates and the “edited by” information.
• Obtain and document the return of all Company property, including the originals and copies of all company information, whether in hard copies or electronically stored.

• Obtain and document the return of all company-owned electronic devices (smart phones, tablets, laptops, thumb/flash drives, wearable devices, and other technology).

• If company policies permit have the departing employee produce all company-paid for or personally owned electronic devices used for company purposes for inspection and deletion of company information and trade secrets.

• Review the status of the employee’s agreements with the company, including the annual acknowledgment of the company’s policies. If any acknowledgments are missing, ask the employee to sign an acknowledgment during the exit interview.

• Any separation or severance agreement must contain a provision in which the departing employee re-affirms his/her obligations under any previously signed confidentiality/non-disclosure agreements followed by a provision providing the Notice of the Immunity provisions of the Defend Trade Secrets Act (or cross-referencing a previously signed agreement or policy providing the required DTSA Notice).

• Schedule an exit interview with a human resources representative and with the employee’s manager upon confirming the employee’s departure.

• If management suspects theft of trade secrets or confidential information, immediately arrange for forensic imaging of the hard drive of the employee’s computer and all company-owned electronic devices.

• Send letter to employee after departure reminding him of his or her obligations under any agreements he or she signed.

• Send letter to new employer after departure informing it of the agreements the employee signed.