

# NAPBS 2010 ANNUAL CONFERENCE

SAN ANTONIO, TEXAS

MARRIOTT SAN ANTONIO RIVERCENTER

MARCH 7-9

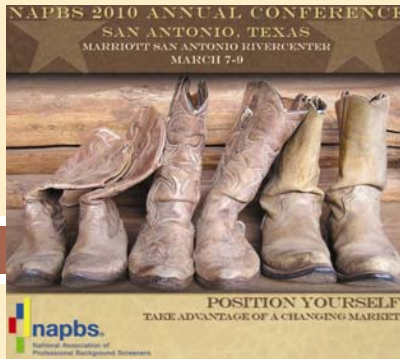


**POSITION YOURSELF**

**TAKE ADVANTAGE OF A CHANGING MARKET**



National Association of  
Professional Background Screeners



# Covering Your Assets: Identifying And Protecting Your Trade Secrets

Presented by:  
Ron S. Brand, Esq.

FISHER & PHILLIPS LLP  
ATTORNEYS AT LAW

[rbrand@laborlawyers.com](mailto:rbrand@laborlawyers.com)

[www.laborlawyers.com](http://www.laborlawyers.com)

- ATLANTA • BALTIMORE • CHARLOTTE • CHICAGO • COLUMBIA • DALLAS • DENVER •
- FORT LAUDERDALE • HOUSTON • IRVINE • KANSAS CITY • LAS VEGAS • LOUISVILLE •
- NEW JERSEY • NEW ORLEANS • ORLANDO • PHILADELPHIA • PHOENIX • PORTLAND (MAINE) •
- PORTLAND (OREGON) • SAN DIEGO • SAN FRANCISCO • TAMPA •

# Economic Espionage Has Become A Multibillion Dollar Industry

- *“Economic espionage is the unlawful or clandestine targeting or acquisition of sensitive financial, trade, or economic policy information; proprietary economic information; or critical technologies.”* U.S. Attorney General Office, The 2002 Annual Report to Congress on Foreign Economic Espionage and Industrial Espionage.
- Statistics drawn from various industry and government sources show that losses due to economic espionage, including trade secrets theft, are estimated at more than \$150 billion a year.

# Economic Espionage Has Become A Multibillion Dollar Industry

- Symantec Corp. survey conducted in 2009.
  - Found that the theft of trade secrets and confidential customer information cost companies an average of \$2 million.
  - 75% of the 2,100 information technology executives surveyed reported cyber attacks, with most of the intrusions aimed at stealing a company's trade secrets, such as product strategies and designs.
- Ponemon Institute survey conducted in 2009.
  - Found that nearly 60% of employees who resigned or were terminated stole company data.
    - 65% of those employees stole e-mail lists.
    - 49% of those employees stole non-financial business information.
    - 39% of those employees stole customer contact lists.
    - 35% of those employees stole personnel records.
    - 16% of those employees stole financial information.

# Economic Espionage Has Become A Multibillion Dollar Industry

- According to Dan Swartwood (current Director of Information Safeguarding at the Walt Disney Company and former Corporate Information Security at the Compaq Computer Corporation) at a Congressional sub-committee hearing on corporate espionage in 2000:
  - Less than 3% of all information technology and security dollars are spent protecting or safeguarding electronic or hard copy confidential information.
  - The vast majority of these dollars are spent on physical and electronic measures designed to keep outsiders from penetrating corporate networks.
  - Little is done to protect confidential information from either the untrained or disgruntled employee.

# Economic Espionage Has Become A Multibillion Dollar Industry

- What are the thieves after?
  - *Customer lists.*
  - Financial data.
  - Research and development work.
  - Merger and acquisition plans.
  - Unannounced product specifications and prototypes.
  - Computer source code/software.
  - Engineering plans and drawings.
  - Biomedical research.
  - Sales forecasts.

# Economic Espionage Has Become A Multibillion Dollar Industry

- The thieves of trade secrets can be:
  - Current disgruntled employees.
  - Former employees about to go to work for competitors.
  - Competitors.
  - Vendors/suppliers.
  - Government agencies.
- According to the American Society for Industrial Security, an international organization for security professionals:
  - More than 75% of thieves are employees or contractors.
  - Another 6% or more are domestic competitors.
  - Only 7% steal secrets on behalf of foreign companies or governments.

# Economic Espionage Has Become A Multibillion Dollar Industry

- Trade secrets can be stolen from:
  - File cabinets.
  - Rolodexes.
  - Employee personnel files.
  - Computers and servers.
  - Internet.
  - E-mail.
  - Off-site login.
  - Cyber attacks.
  - High-tech surveillance equipment.
  - Cell phones/PDAs.
  - Fax machines.
  - Garbage.

# Economic Espionage Has Become A Multibillion Dollar Industry

- The Ponemon Institute survey found:
  - 61% of employees who stole company data did so through old-fashioned theft of paper documents or hard files.
  - 52% of employees who stole company data downloaded the information onto a disc.
  - 42% of employees who stole company data downloaded the information onto a USB memory stick.
  - 38% of employees who stole company data sent the information from their work e-mail accounts to personal e-mail accounts.
  - 25% of employees who stole company data indicated that they were able to access the information on a company's computer network even after they had departed.

# Defining A Trade Secret: Finding The Diamond In The Rough

- What is a trade secret?
  - The federal Uniform Trade Secrets Act (UTSA), which has been adopted by most states, defines a trade secret as information including a formula, pattern, compilation, program, device, method, technique or process that:
    - 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 use and disclosure.
    - Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

# Defining A Trade Secret: Finding The Diamond In The Rough

- What type of information has “independent economic value”?
  - ▣ Information that provides a “substantial business advantage” because of its secrecy.
- What does “information not generally known” mean?
  - ▣ Information that has not yet been ascertained by others in the industry (those to whom the information would be of economic benefit).

# Defining A Trade Secret: Finding The Diamond In The Rough

- What types of information can be trade secrets?
  - Customer lists – usually not just names and addresses, but preferences and buying habits.
  - Contract information.
  - Supplier/vendor information.
  - Marketing information.
  - Business development strategy.
  - Employee personnel information.
  - Formulas/inventions.
  - Technical processes.
  - Financial records.

# Defining A Trade Secret: Finding The Diamond In The Rough

- You should not be overzealous in what information you consider to be a trade secret.
  - ▣ Not all information can be protected as a trade secret.
    - Only information that has independent economic value because it's not generally known in the industry, and has been treated as confidential, is a trade secret.
- Information that is not a trade secret can still be confidential, but remedies offered by the Uniform Trade Secrets Act (such as the ability to recoup attorneys' fees) may not be available.

# Defining A Trade Secret: Finding The Diamond In The Rough

- What constitutes “misappropriation” of trade secrets?
  - Essentially the acquisition, use or disclosure of a trade secret through “improper means” or knowledge that someone else acquired the trade secret through “improper means.”
  - No physical taking required; can be information in someone’s head.
  - Even an innocent use or disclosure of another’s trade secrets may be actionable.
- What does “improper means” mean?
  - Acquisition of a trade secret by “improper means” includes theft, bribery, misrepresentation, breach or inducement of a breach of duty to maintain secrecy, or espionage through electronic or other means.
  - It is not improper to discover a competitor’s trade secrets by fair and honest means, such as through reverse engineering.

# Treat A Diamond Like A Diamond: How To Protect Your Trade Secrets

- One of the best methods to help ensure that your confidential information will be recognized as trade secrets is to implement a proactive trade secrets protection program.
- An effective trade secrets protection program generally includes the following components:
  - ▣ Identifying the trade secrets in your domain and categorizing the relative value of the information.
  - ▣ Addressing employment relationships.
  - ▣ Securing the physical environment.
  - ▣ Managing and securing access to your trade secrets.
- The optimal approach for implementing a trade secrets protection program is through the formation of a team that will be in charge of identifying your trade secrets and implementing the program.

# Treat A Diamond Like A Diamond: How To Protect Your Trade Secrets

## □ **Addressing employment relationships.**

- Utilize confidentiality agreements, non-solicitation agreements, non-compete agreements, and agreements that assign to you any “inventions” created by an employee during the course of his or her employment.
  - Keep in mind that the standard for enforceability of such agreements varies by state, and some states (like California) prohibit non-compete agreements outright.

# Treat A Diamond Like A Diamond: How To Protect Your Trade Secrets

- When looking to enforce such agreements, remember the following:
  - *The burden is on you.* Assume your agreement will be painted as an unlawful restraint on trade and an illegal restriction, and assume that a court will look for any opportunity to hold it invalid.
  - *One size does not fit all.* Carefully draft all agreements to protect only legitimate business interests, and closely follow the legal requirements of whatever state law will control if the agreement is ever enforced or challenged.

# Treat A Diamond Like A Diamond: How To Protect Your Trade Secrets

- Implement measures to inform current employees and new-hires of their obligation to protect your trade secrets. References to this obligation can be made in training sessions, employee handbooks, and policy and procedure manuals.
- When terminating employees, remind them during exit interviews of their continuing duty to not use or disclose your trade secrets. Consider using a checklist for returning company equipment, keys and confidential material. Also consider using a termination certificate.

# Treat A Diamond Like A Diamond: How To Protect Your Trade Secrets

## □ Securing the physical environment.

- Implement outside security measure like fencing, lighting, alarms and guards.
- Restrict access to servers, routers and other network technology to those whose job responsibilities require access.
- Keep wire closets, server rooms, phone closets and other locations containing sensitive equipment locked at all times.
- Place locks on computer cases to prevent hardware tampering.
- Designate all documents containing trade secrets or confidential information as “confidential” and implement procedures to help ensure that all documents deserving the “confidential” designation are appropriately marked when initially created.
- Implement a process for destroying rather than just discarding obsolete trade secrets or confidential information which could still damage your company if it fell into a competitor’s hands.

# Treat A Diamond Like A Diamond: How To Protect Your Trade Secrets

- **Managing and securing access to your trade secrets.**
  - Utilize inside computer security measures, such as:
    - Implementing passwords for all employees.
    - Monitoring and logging employees' computer and internet actions.
    - Keeping audit logs of all access requests to your company's computer systems.
    - Using a firewall.
    - Auditing the servers for security holes.
    - Making sure computers have the latest security patches and fixes installed.
    - For highly sensitive trade secrets, even more extraordinary measures should be considered, such as scrambling or encoding messages and computer files.
    - Backing-up all workstations and servers at least weekly, and storing back-ups off-site.

# Treat A Diamond Like A Diamond: How To Protect Your Trade Secrets

- Consider steps to help protect your trade secrets from unauthorized disclosure or use by third parties, such as:
  - Ensuring that contracts and licensing agreements expressly state the parameters for using and disclosing your trade secrets.
  - Ensuring that standard contracts with subcontractors and vendors contain a confidentiality provision.
  - Requiring visitors to sign a non-disclosure agreement before touring your facility or receiving your trade secrets.
  - Training employees not to discuss your trade secrets around third parties.

# Your Trade Secrets Have Been Stolen: What Can/Should You Do?

- Consider the following scenario:
  - One of your key employees with knowledge of your valuable trade secrets has announced that he is leaving for a similar position with your company's chief competitor.
  - The day before resigning the employee attended a highly sensitive presentation that discussed your company's competitive strategy for the next several years, during which sensitive documents were distributed to the attendees.
  - Your business could be devastated if the employee were to disclose your trade secrets to your chief competitor, and/or use your trade secrets to compete against you.

# Your Trade Secrets Have Been Stolen: What Can/Should You Do?

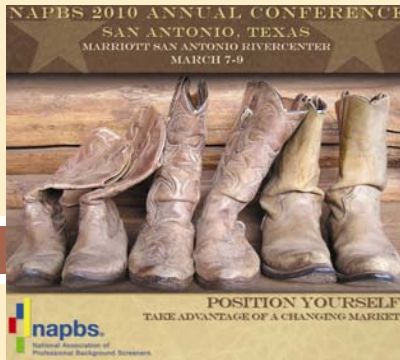
- What can/should you do?
  - Cease and desist/reminder of confidentiality obligation letters.
    - Least expensive alternative.
    - May not be enough though.
  - Criminal prosecution.
    - The element of surprise.
    - Good for highly sensitive, one-of-a-kind information.
    - Loss of control of resolution.
    - Example: Joya Williams sentenced to 8 years in federal prison for stealing trade secrets belonging to Coca-Cola.

# Your Trade Secrets Have Been Stolen: What Can/Should You Do?

- Seek a temporary restraining order and/or preliminary injunction.
  - Used to stop breaching activity.
  - But, you should have evidence of actual or threatened misappropriation of trade secrets, or breach of an agreement before seeking such relief.
  - Bond requirement.
- Sue for monetary damages.
  - Actual or compensatory damages, punitive damages, royalties, attorneys' fees and costs.

# Your Trade Secrets Have Been Stolen: What Can/Should You Do?

- When deciding whether to move forward with litigation to protect your trade secrets, remember to think first, and then act second!
- Stay focused on the objectives you want to achieve.
  - Is there a “middle ground” for settlement that satisfies your primary objectives?
  - Should you first write a cease and desist letter? Should you sue? If you sue, should you move for a temporary restraining order and/or preliminary injunction?
  - What information will you need to disclose to prove your case, and are you willing to reveal your trade secrets during litigation?
  - What are the actual or potential damages if you do not take legal action?
  - What will happen to the relationship with your competitor and/or customers when you sue?
  - Have you considered the legal fees and costs associated with litigating a trade secrets case?



# Covering Your Assets: Identifying And Protecting Your Trade Secrets

Thank You!

Presented by:  
Ron S. Brand, Esq.

FISHER & PHILLIPS LLP  
ATTORNEYS AT LAW

[rbrand@laborlawyers.com](mailto:rbrand@laborlawyers.com)

[www.laborlawyers.com](http://www.laborlawyers.com)

- ATLANTA • BALTIMORE • CHARLOTTE • CHICAGO • COLUMBIA • DALLAS • DENVER •
- FORT LAUDERDALE • HOUSTON • IRVINE • KANSAS CITY • LAS VEGAS • LOUISVILLE •
- NEW JERSEY • NEW ORLEANS • ORLANDO • PHILADELPHIA • PHOENIX • PORTLAND (MAINE) •
- PORTLAND (OREGON) • SAN DIEGO • SAN FRANCISCO • TAMPA •