

Protecting Electronic Data and Trade Secrets

Presenter: Robert W. Kent, Jr.

Baker & McKenzie International is a Swiss Verein with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a “partner” means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an “office” means an office of any such law firm.



Overview

- Basics of trade secret law
- “Reasonable Efforts”
- Reasons to go beyond “Reasonable Efforts”
- The Sentencing Guidelines and trade secrets
- What to do when a key employee leaves



The Basics

- Patents v. Trade Secrets
- Definitions
 - Uniform Trade Secrets Act: information, including a formula, compilation, device or process, that derives independent economic value from not being generally known to, and not being readily ascertainable by proper means by, others who can obtain economic value from its disclosure, and is the subject of efforts that are reasonable under the circumstances to maintain its secrecy
 - Economic Espionage Act (18 USC 1849)
 - Same as UTSA except: (1) required secrecy is from the “public,” and (2) the effort requirement is phrased as “reasonable measures to keep such information secret”
 - Essentially the same



Reasonable Efforts

- Extremely fact driven. Case law not particularly helpful.
- One thing clear: perfect secrecy not required
- Depends on the circumstances
 - Nature of the alleged trade secret
 - How it is stored
 - How it is used
 - Nature of industry
 - Type of company



Reasonable Efforts

- DOJ’s “typical” factors
 - Keeping the secret physically, secure in locked drawers, cabinets, or rooms
 - Restricting access to those with a need to know
 - Restricting visitors to secret areas
 - Requiring recipients to sign confidentiality, nondisclosure or noncompetition agreements
 - Marking documents as confidential or secret
 - Encrypting electronic documents
 - Protecting computer files and directories with passwords
 - Splitting tasks among people or entities to avoid concentrating too much information in one place



Reasons To Go Beyond “Reasonable Efforts”

- Achieving “reasonable efforts” should not be the goal
 - Hard to predict how a court will interpret
 - Being able to sue in the event of trade secret theft is not the only objective
- Trade secrets are most valuable when not stolen



U.S. Sentencing Guidelines

- The “Gold Standard” of compliance programs
- Risk assessment
- Tone at the top
- Policies and procedures
- Training
- Auditing and reporting
- Enforcement and discipline
- Due diligence on employees and contractors



Risk Assessment

- Identify which information should be protected
- Apply classifications
- Determine perceived risks
 - Outsider theft, departing employees, third parties, natural disaster
- Determine likelihood of each perceived risk
- Determine potential loss associated with each risk
- Identify and evaluate existing policies
- Determine risk tolerance of company
- Determine resource availability and costs of solutions



Tone At The Top

- Real risk assessment will not happen without it
- Senior management statements
- Senior management and board training
- Senior management makes clear that compensation depends on compliance



Policies and Procedures

- Code of Conduct should refer to intellectual property
- Every employee should sign a confidentiality agreement
 - Agreement should identify the trade secrets
- Every third party to whom trade secrets are disclosed should sign a nondisclosure agreement
- Confidential materials should be marked as such
 - Do not overuse the “Confidential” stamp



Policies and Procedures

- Implement appropriate “facilities” measures
 - Perimeter security
 - Building and room security
 - Visitor security
 - Signage
 - Technology and personnel assigned to keep track of distribution
 - Shredders
 - Exit interviews



Policies and Procedures

- Implement appropriate computer protections
 - Firewall on network
 - Passwords
 - Encryption
 - Need to know access
 - Restrictions on printing
 - Restrictions on emailing



Training

- For many companies, employee mistakes are the biggest risk
- Repetition is key
- Creativity is key



Auditing, Reporting and Discipline

- Review to make sure procedures are being followed
- Use technology as appropriate to monitor
- Incorporate trade secret compliance into compensation decisions
- Report results to decisionmakers
- Implement appropriate sanctions in response to discovered noncompliance



Due Diligence

- Thieves and spies
 - Your corporation as victim
 - Your corporation as perpetrator



What To Do When A Key Employee Departs

- Have a plan in place beforehand
- Identify the trade secrets in jeopardy
- Review the employee's confidentiality agreement
- Exit interview
 - Explain your concern and his obligations
 - Identify the trade secrets
 - Ask him to describe in writing his future employment and how he can perform while honoring his obligations
 - Remind him of obligation to return all materials



What To Do When A Key Employee Departs

- Consider whether to contact the new employer
 - Ask for description of duties
 - Ask for plan re avoidance of trade secret disclosure
- Interview remaining employees to see if they know anything
- Consider litigation
 - Trade secret theft, breach of contract, breach of fiduciary duty
 - “Inevitable” trade secret theft
- Consider reporting the situation to law enforcement



Questions

Robert W. Kent, Jr.
Baker & McKenzie LLP
One Prudential Plaza
Chicago, IL 60601
(312) 861-8077
robert.w.kent@bakernet.com