October 19, 2016

Schiff Hardin’s Labor and Employment Group presents:

Protecting Employer Confidential Information

Presenters

Julie J. Stahr
Partner
Schiff Hardin LLP, Chicago
Ms. Stahr is an experienced litigator and counselor representing management in employment-related matters in state and federal court and administrative agencies. Her work includes discrimination, harassment and retaliation claims, defamation, public policy and other tort and common law claims, employment contract and severance claims, reductions in force, restrictive covenants and trade secrets issues, and wage and hour. She is a frequent speaker and presenter in a variety of forums and frequent writer on topical issues, and frequently invited to train on-site on topics of interest to her clients’ workforces. Ms. Stahr is Editor of Schiff Hardin’s Employment Law Landscape blog.

Matthew F. Prewitt
Partner
Schiff Hardin LLP, Chicago
Mr. Prewitt is Chair of the firm’s Cybersecurity and Data Privacy Team and Co-Chair of the firm’s Trade Secrets and Employee Mobility Team. He is a trial lawyer with a national practice litigating claims arising from the theft or misuse of confidential information and trade secrets. Mr. Prewitt is an adjunct professor of law at Chicago-Kent Law School, where he teaches a course on the law of data security and data privacy. He is an active participant in The Sedona Conference, Working Groups 1 and 11, where his work includes serving on the drafting team for a forthcoming paper on “bring your own device” law and policy issues and a data privacy law primer. He is a Certified Information Privacy Professional (CIPP-US).
Evolving Issues In Trade Secrets Law

Defend Trade Secrets Act

18 USC §1831 et seq. (Amending Economic Espionage Act)

Creates a New Federal Civil Claim for Trade Secret Misappropriation
- federal subject matter jurisdiction, nationwide service of process, subpoenas, discovery, enforcement of orders and judgments

Does Not Preempt State Law
- injunctions may not “conflict with an applicable state law prohibiting restraints on the practice of a lawful profession, trade or business”

Defend Trade Secrets Act

“Inevitable disclosure” not available

Injunctions may place restrictions on the work to be performed, but the restrictions “shall be based on evidence of threatened misappropriation and not merely on the information the person knows”
Defend Trade Secrets Act

A new statutory procedure for *ex parte* seizures

- “Extraordinary circumstances”
- Destruction / dissemination must be imminent if notice is given
- Court retains custody of seized materials
- Court may appoint special master
- Data safeguards (no access, no connection to internet/network, encryption)
- Plaintiff must provide bond and may be subject to damages for wrongful seizure

Defend Trade Secrets Act

Limited Immunity

- Immunity from liability from trade secrets disclosure in specified circumstances
  - For trade secrets disclosures made in confidence to attorney / government official solely for purpose of reporting or investigating suspected violation of law
  - For trade secrets disclosure made in a filing in a lawsuit or “other proceeding” under seal
  - If filing a retaliation lawsuit against employer for reporting suspected violation of law, can disclose trade secrets to employee’s attorney for use in the proceeding under seal, with no other disclosure

Notice requirement for employer confidentiality agreements

- No exemplary damages or attorneys' fees/costs for any employer that does not provide notice of DTSA's immunity provisions
Defend Trade Secrets Act

The Essential Elements of a Trade Secret Remain Unchanged

The term “trade secret” means all forms and types of financial, business, scientific, technical, economic, or engineering information . . . 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.

Evolving Issues In Trade Secrets Law

Heightened Awareness and Regulation of Data Security and Data Privacy Are Transforming Trade Secret Protection
Employer Tools

- Employment agreements
- Employment policies
- Separation agreements
- Departing employee procedures
- Other suggested protocols

Employer Tools

Employment Agreements

1. Confidential information clauses
   - consider a temporal restriction for non-trade secret information
   - define confidential information as specifically as possible (note increasing scrutiny on scope of confidential information clauses)
   - recitals acknowledging necessity of confidential information restrictions
   - note the 2-year rule in IL – unclear how applied to confidential information clauses
Employer Tools

Employment Agreements

2. **Departing employee obligations**
   - inspection of personal devices used for work
   - return of information
   - agreement to participate in exit interview
   - notification to subsequent employers of confidentiality obligations
   - notification to current employer of all employment within specified period of time after departure
   - consider inevitable disclosure-based restriction

3. **Invention assignment clause**
   - inform company of patent applications and inventions for specified period of time after departure
   - authorize company to act as agent for assignment

4. **Use of company electronic information and systems**
   - no expectation of privacy
   - no installation of software or programs without approval
   - no non-company related use of company information
   - statement regarding download, access, saving of company information on personal devices
5. *Bring your own device clause*
   - monitoring and use of company content/information
   - data encryption/password protection
   - wiping of data upon employee departure or if device lost or stolen (with obligation to notify)
   - inspection of device upon request
   - installation of software deemed necessary for protection of company information

6. **DTSA notice requirement**
   - applies to any contract with an employee that addresses confidentiality
   - NDAs, employment agreements, severance agreements, settlement agreements, BYO equipment agreements, etc.
   - broad application: “employee” includes independent contractors, consultants
   - no exemplary damages or attorneys’ fees/costs for any employer that does not provide notice
   - Employee must be notified of immunity from liability:
     1) for trade secrets disclosures made in confidence to attorney / government official solely for purpose of reporting or investigating suspected violation of law;
     2) for trade secrets disclosure made in a filing in a lawsuit or “other proceeding” under seal;
     3) if filing a retaliation lawsuit against employer for reporting suspected violation of law, can disclose trade secrets to employee’s attorney for use in the proceeding under seal, with no other disclosure
Employer Tools

Employment Agreements

Sample DTSA notice:

You are hereby notified that you will not be held criminally or civilly liable under any federal or state trade secret law for the disclosure of a trade secret that (A) is made (i) in confidence to a federal, state, or local government official, either directly or indirectly, or to an attorney; and (ii) solely for the purpose of reporting or investigating a suspected violation of the law or (B) is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal. Additionally, an individual who files a lawsuit for retaliation by an employer for reporting a suspected violation of law may disclose the trade secret to the attorney of the individual and use that information in the court proceeding only if the individual files any documents containing the trade secret information under seal and does not disclose the trade secret, except pursuant to court order.

Employer Tools

Employment Policies

1. Confidential information
2. Proper use of company electronic information, devices and systems
3. Standards of conduct policy - include information security
4. Performance evaluation policy – include information security
5. Provide notice of electronic monitoring
6. Exit interview
   • Cannot typically enforce employment policies after an employee’s departure, but useful to provide notice of expectations, support disciplinary measures during employment, and help demonstrate “reasonable measures” to protect information
**Employer Tools**

**Separation Agreements**

1. Impose post-employment confidentiality obligations
2. Re-affirm prior confidentiality obligations
3. Affirmations regarding non-use, non-possession and return of information
4. Material terms; severance clawback (age waiver should have separate consideration not subject to clawback)
5. Opportunity to provide DTSA notice if missing from prior employment agreement (sufficiency of after-the-fact notice unclear)
6. If new employer is known, affirmations that new employer has been notified of employee’s confidentiality obligations

**Employer Tools**

**Departing Employee Protocols**

1. Exit interview
2. Review recent email traffic
3. Image computers when warranted
4. Consider freeze on use of hardware and devices for a period of time
**Employer Tools**

**Other Suggested Protocols**

- Password protection
- Access to limited user groups
- Electronic monitoring (notice, consistency, non-discrimination)
- Reminders of contractual obligations and employment policies during annual reviews or other regularly scheduled communication
- Enforcement of contractual obligations and employment policies as protection and deterrent
  - Note enforcement difficulties - consistency v. fact specific necessity
  - Approach should be aligned for employees with similar positions or levels of access to information

---

**Employee Buy-In**

- Implement reasonable policies that are easy to understand and compliance is achievable
- Communicate the importance of the policies/requirements to the success of the company: we are in this together
- Messaging:
  - It is the right thing to do
  - Not a “victimless crime”
  - We do this because it matters
  - We enforce when there’s good reason to
- Quid pro quo for employment agreements – employment terms, bonuses, severance
Julie J. Stahr

Julie is sought after as an advisor and litigator by clients large and small who want effective, real-world counsel and solutions to the personnel issues employers face on a daily basis. Julie is an experienced litigator and counselor representing management in employment-related matters in state and federal court and administrative agencies. Her work includes discrimination, harassment and retaliation claims, tort claims such as defamation, public policy and common law claims, employment contract and severance claims, reductions in force, claims involving restrictive covenants and trade secrets; and wage and hour claims. When it comes to looking down the road for her clients, Julie is astute. She can anticipate potential issues or risks that may arise based on decisions made today.

Julie is a frequent speaker and presenter in a variety of forums and frequent writer on topical issues. She brings a common sense, practical approach to public speaking in settings both large and small. She has been a featured presenter in such forms as the American Bar Association, the Practicing Law Institute, the National Retail Federation, the Business Women’s Professional Group, Council on Education in Management, the Latin American Chamber of Commerce, and other organizations, as well as a recurring presenter at Schiff Hardin client briefings and seminars. In addition, clients frequently ask Julie to train and present topics on site on topics of interest to their workforce.

Education

• DePaul University College of Law, J.D., 1993
• University of Illinois at Urbana-Champaign, B.A., 1990

Bar Admissions

• Illinois
• California
• U.S. Court of Appeals for the Third Circuit
• U.S. Court of Appeals for the Seventh Circuit
• U.S. District Court for the Northern District of Illinois
• U.S. District Court for the Northern District of Florida

Awards & Honors

• Client Service All-Star, BTI Consulting Group (2015)
• Peer Reviewed AV® Preeminent™, Martindale-Hubbell (Since 2007)

Matthew F. Prewitt

Matthew F. Prewitt is a trial lawyer with a national practice in trade secrets litigation and disputes arising from misuse of confidential information and from breach of noncompetition agreements and other restrictive covenants. As lead trial counsel, Matt has obtained injunctive relief in expedited proceedings in more than a dozen states. He has extensive experience investigating and trying complex claims for theft and destruction of electronic data and has won case-terminating sanctions for destruction of electronic data in multiple suits. Matt also counsels clients on corporate information governance for competitive information, providing advice that integrates the law of trade secrets, data privacy, and cybersecurity.

Matt also won what was reported in the legal press as the first award of a defendant’s entire fees for multiyear trade secrets litigation under the Illinois Trade Secrets Act, persuading the court that the plaintiff had brought the suit in bad faith.

As a trial lawyer who regularly leads the prosecution and defense of complex, fast track injunction proceedings, Matt has learned how to triage the potential factual and legal issues to develop a focused, winning strategy that achieves the client’s business objectives. Because Matt’s clients frequently look to him to bring suit to protect intellectual property rights, Matt knows how to litigate as a plaintiff, by seizing the initiative and framing the issues for trial.

Matt frequently applies these skills in “rescue” engagements where he is called upon to augment or replace prior trial counsel at an advanced stage of the case. These engagements have provided Matt substantive experience in a broad range of business, environmental, and mass tort disputes in both the trial courts and in bankruptcy proceedings.

Matt is a Certified Information Privacy Professional (CIPP-US). He is also an adjunct professor of law at Chicago-Kent College of Law and an active participant in The Sedona Conference Working Group 1 (Electronic Document Production and Retention) and Working Group 11 (Data Security and Privacy Liability). He is a member of the International Association of Privacy Professionals.