Protecting Corporate Assets from Departing Employees

by

Robert B. Fitzpatrick
rfitzpatrick@robertbfitzpatrick.com



BIOGRAPHY

- Robert ("Bob") Brian Fitzpatrick is the principal in the law firm of Robert B. Fitzpatrick PLLC in Washington, D.C. where represents clients in employment law matters. Mr. Fitzpatrick has concentrated his practice in employment law disputes for more than fifty years. He has represented clients in individual and class actions. He has represented clients in employment discrimination, workplace harassment, retaliation, age discrimination, FMLA, ADA, whistleblower, wrongful termination, non-compete, trade secrets, Computer Fraud and Abuse Act, and wage and hour claims, among others. He counsels numerous executive clients regarding employment agreements and compensation issues. He has negotiated literally thousands of severance agreements. He is also a frequent speaker on employment law topics, and has written countless articles on employment law, a few of which can be found on his website and his blog, Fitzpatrick on Employment Law.
- Prior to entering private practice, Mr. Fitzpatrick served as a staff attorney in the Jackson, Mississippi office of the Lawyers' Committee for Civil Rights Under Law in the late 1960's; as a staff attorney in the Office of General Counsel of the Equal Employment Opportunity Commission in the early 1970's; and with the Washington Research Project (now the Children's Defense Fund) training minority attorneys in the Deep South to litigate employment discrimination cases. He has been in private practice in Washington, D.C. since 1970. He is an avid hiker and kayaker. He is a Fellow of the College of Labor & Employment Lawyers, having been inducted as a Fellow at the first annual induction ceremony in 1996. He has been listed as one of The Best Lawyers in America® for at least 25 continuous years.
- He is admitted to practice in all courts of the District of Columbia (Superior Court, D.C. Court of Appeals, and the Federal District Court of the District of Columbia), the Federal District Court for Maryland, the Federal District Court for the Northern District of Mississippi, the Supreme Court of the United States, the Federal Circuit, the Court of Federal Claims, and the United States Courts of Appeals for the District of Columbia as well as the Fourth and Sixth Circuits.

DISCLAIMER OF ALL LIABILITY AND RESPONSIBILITY

THE INFORMATION CONTAINED HEREIN IS BASED UPON SOURCES BELIEVED TO BE ACCURATE AND RELIABLE – INCLUDING SECONDARY SOURCES. DILIGENT EFFORT WAS MADE TO ENSURE THE ACCURACY OF THESE MATERIALS, BUT THE AUTHOR ASSUMES NO RESPONSIBILITY FOR ANY READER'S RELIANCE ON THEM AND ENCOURAGES READERS TO VERIFY ALL ITEMS BY REVIEWING PRIMARY SOURCES WHERE APPROPRIATE AND BY USING TRADITIONAL LEGAL RESEARCH TECHNIQUES TO ENSURE THAT THE INFORMATION HAS NOT BEEN AFFECTED OR CHANGED BY RECENT DEVELOPMENTS.

THIS PAPER IS PRESENTED AS AN INFORMATIONAL SOURCE ONLY. IT IS INTENDED TO ASSIST READERS AS A LEARNING AID; IT DOES NOT CONSTITUTE LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL ADVICE. IT IS NOT WRITTEN (NOR IS IT INTENDED TO BE USED) FOR PURPOSES OF ASSISTING CLIENTS, NOR TO PROMOTE, MARKET, OR RECOMMEND ANY TRANSACTION OR MATTER ADDRESSED; AND, GIVEN THE PURPOSE OF THE PAPER, IT MAY OMIT DISCUSSION OF EXCEPTIONS, QUALIFICATIONS, OR OTHER RELEVANT INFORMATION THAT MAY AFFECT ITS UTILITY IN ANY LEGAL SITUATION. THIS PAPER DOES NOT CREATE AN ATTORNEY-CLIENT RELATIONSHIP BETWEEN THE AUTHOR AND ANY READER. DUE TO THE RAPIDLY CHANGING NATURE OF THE LAW, INFORMATION CONTAINED IN THIS PAPER MAY BECOME OUTDATED. IN NO EVENT WILL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, OR OTHER DAMAGES RESULTING FROM AND/OR RELATED TO THE USE OF THIS MATERIAL.

Practical Tips to Handle Departing Employees Pre and Post Termination

“One Piece at a Time”
Johnny Cash

- Well, I left Kentucky back in '49
  An' went to Detroit workin' on a 'sembly line
  The first year they had me puttin' wheels on cadillacs

  Every day I'd watch them beauties roll by
  And sometimes I'd hang my head and cry
  'Cause I always wanted me one that was long and black.

  One day I devised myself a plan
  That should be the envy of most any man
  I'd sneak it out of there in a lunchbox in my hand
  Now gettin' caught meant gettin' fired
  But I figured I'd have it all by the time I retired
  I'd have me a car worth at least a hundred grand.

  [CHORUS]
  I'd get it one piece at a time
  And it wouldn't cost me a dime
  You'll know it's me when I come through your town
  I'm gonna ride around in style
  I'm gonna drive everybody wild
  'Cause I'll have the only one there is a round.

  So the very next day when I punched in
  With my big lunchbox and with help from my friends



- **I left that day with a lunch box full of gears**
  Now, I never considered myself a thief
  GM wouldn't miss just one little piece
  Especially if I strung it out over several years.

Preventative Measures



Using Restrictive Covenants: Keep Agreements Jurisdiction-Specific

Some State Laws Regarding Non-Competes

- California (Cal. Bus. & Prof. Code § 16600): Many non-competes are unenforceable
- Nevada (NRS 613.200): Potential Criminal Penalties
- Connecticut bill (H.B. 6658, 2013 Leg. Sess. (Conn. 2013)): Notification & Review Period



Using Restrictive Covenants: Keep Agreements Jurisdiction-Specific

Some State Computer-Abuse Statutes

- Maryland - Md. Code Ann. Crim. Law § 7-302 (Lexis 2013)
- California - Cal. Penal Code § 502 (Deering 2013)
- Delaware - 11 Del. C. § 931 (Lexis 2013)



Using Restrictive Covenants: Keep Agreements Up-to-Date

- Changes to the employee's job can void non-competes:
  - Promotions
  - Updated Compensation
  - Job Transfers



Using Restrictive Covenants: Keep Agreements Up-to-Date

- Changes to the employer can void non-competes:
  - New Entity
  - Change in Control
  - Location Change
  - *Grace Hunt IT Solutions, LLC v. SIS Software, LLC, et al.*, 29 Mass. L. Rep. 460 (2012)
- Sometimes this can be addressed via contract:
  - *TEKSystems, Inc. v. Fletcher*, Civ. No. 10-11452011 U.S. Dist. LEXIS 22227 (D. Md. Mar. 2, 2011)

Using Restrictive Covenants: Scope of Job Restrictions

- Excessive restrictions on work employee can perform in the future are unenforceable:
  - Work/responsibilities actually performed for employer
  - Unique, specialized skills



Using Restrictive Covenants: Geographic Scope

- Geographic region
  - Reasonably necessary for the protection of the employer
  - Limited to regions where employer does business
  - Limited to regions where employer has customers

Using Restrictive Covenants: Duration

- Duration should be reasonable to protect employer's interests.
- Two approaches:
  - Time needed to hire & train replacement
  - Duration of departing employee's "competitive edge"

Using Restrictive Covenants: Non-Solicit Agreements

- Non-solicits are often viewed more favorably by courts than non-competes
- They will still be struck down if overbroad
  - *Newport Capital Group, LLC v. Loehwing*, Civ. No. 11-2755, 2013 U.S. Dist. LEXIS 44479 (D.N.J. Mar. 28, 2013) (Overbroad definition of a "prospective customer")



Using Restrictive Covenants: Provide for Forfeiture and Clawbacks

- Forfeiture/Employee Choice Doctrine
  - Employee forfeits deferred compensation if employee makes "genuine and knowing voluntary choice" to violate non-compete agreement
  - *Morris v. Schroder Capital Mgmt.*, 859 N.E.2d 503 (N.Y. 2006)
  - *Lucente v. Int'l Bus. Machines Corp.*, 310 F.3d 243 (2d Cir. 2002)

Using Restrictive Covenants: Provide for Forfeiture and Clawbacks

- Clawbacks
  - Recovery of paid or unpaid compensation permitted if employee breaches fiduciary duty
  - *Janssens v. Freedom Med., Inc.*, Civ. No. 10-2042, 2011 U.S. Dist. LEXIS 46670 (D. Md. April 29, 2011)

Policies

- Develop policies to address problem areas:
  - Computer Use
  - Network authorization
  - Passwords
  - Remote Access/Remote Computing
  - System Administrators
  - Federal Contractors

Limit Access:
Ensure the Secrecy of Confidential Information



- Uniform Trade Secrets Act:
  - Information is not generally known; and
  - "is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."

Limit Access:
Ensure the Secrecy of Confidential Information

- To enforce, secrets must be identified with "reasonable particularity"
- Bottom line: make good use of passwords and policies to prohibit employee access to files without authorization

Limit Access:
Limit Authorization to Access Important Company Information

- The Computer Fraud & Abuse Act ("CFAA")
  - Accessing a computer without authorization
  - Exceeding authorized access
  - Requires a showing of damage or loss

Limit Access:
Limit Authorization to Access Important Company Information

- Fourth and Ninth Circuits have a narrow definition of "unauthorized access".
  - *United States v. Nosal*, 676 F.3d 854, 857 (9th Cir. 2012)
  - *WEC Carolina Energy Solutions, LLC v. Miller et al.*, 687 F.3d 199 (4th Cir. 2012), *cert. dismissed,* 133 S.Ct. 831 (2013)

Limit Access:
Limit Authorization to Access Important Company Information

- The First and Third Circuits have a broad definition of "unauthorized access":
  - *EF Cultural Travel BV v. Explorica, Inc.*, 274 F. 3d 577 (1st Cir. 2001)
  - *U.S. v. Tolliver*, 451 Fed. Appx. 97 (3d Cir. 2011)

Limit Access: Passwords

- Effective Password Management:
  - Have a written policy
  - Don’t write passwords down
  - Store passwords digitally in a secure location

Limit Access: Passwords

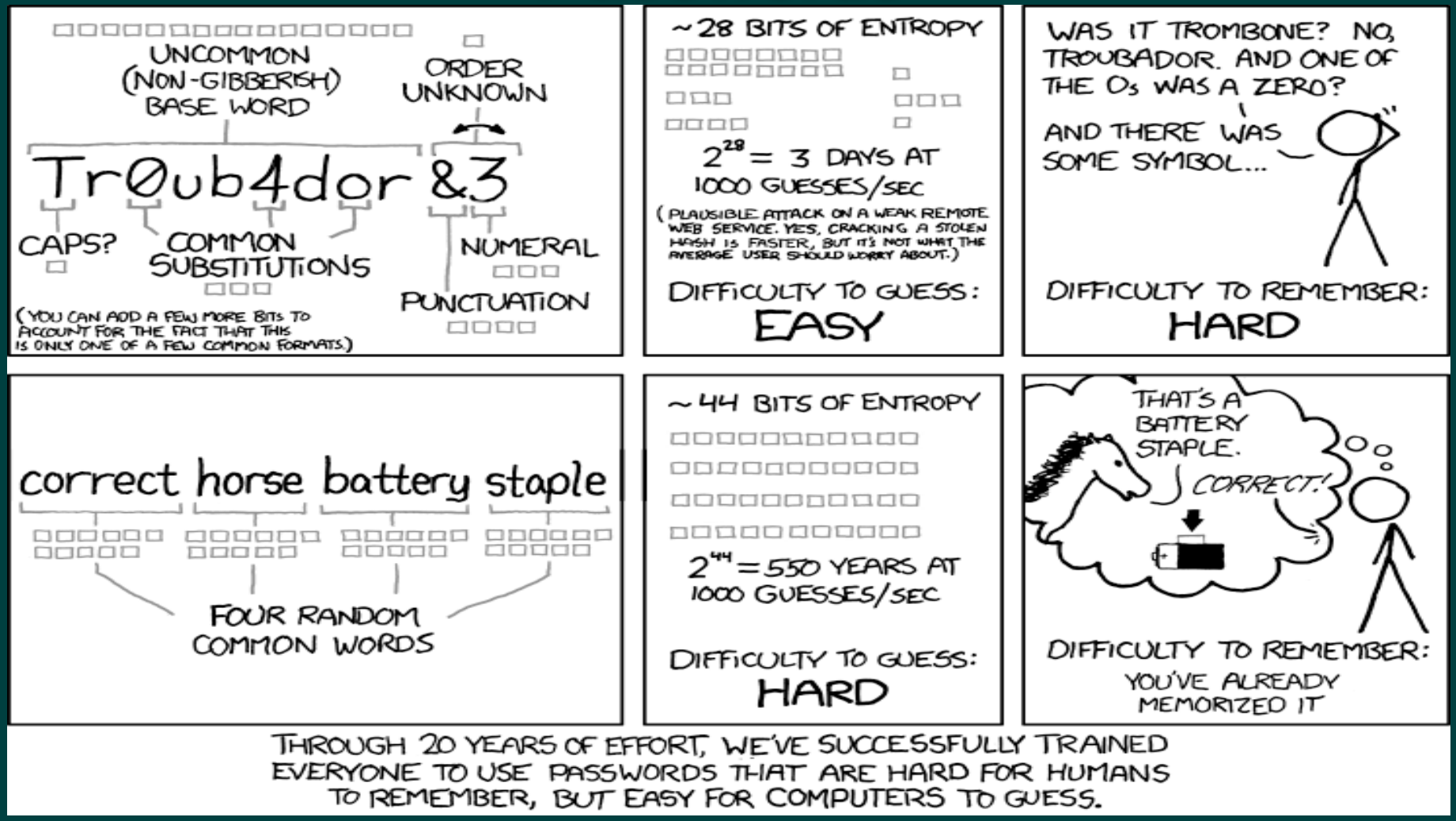


- Hallmarks of a strong password:
  - Use letters (upper and lower case), numbers, and symbols
  - Do not use dictionary words
  - Eight or more characters long
  - Change passwords regularly (every 2-3 months)
  - Never write your password down or save it on your computer

Limit Access: Passwords

- How to remember strong passwords:
  - Use the first letter of each word of a long phrase interspersed with symbols and numbers
  - Use a long phrase as your password. Windows can support up to 127 character passwords. A sufficiently long phrase is a strong password even if it contains dictionary words (e.g. “This is My 3rd New password this Year!”)

Limit Access: Passwords



Courtesy: xkcd.com/936/

Limit Access:
HMV – An Object Lesson



- "The lesson for any business is clear: If you're facing an uncomfortable collision with loyal employees, lock down your social media accounts. The anonymous worker indicated in another series of tweets … that HMV's feeds were set up by an intern years ago and likely not secured."
  - Jared Keller, "HMV Employee Commandeers Corporate Twitter Account in Response to Layoffs," BusinessWeek, Jan. 31, 2013, http://www.businessweek.com/articles/2013-01-31/hmv-employees-commandeer-corporate-twitter-account-in-response-to-layoffs

Limit Access: Social Media

- Carefully define ownership and scope of use of social media accounts:
  - *PhoneDog v. Kravitz*, Civ. No. 11-03474, 2011 U.S. Dist. LEXIS 129229 (N.D. Cal. Nov. 8, 2011)
  - *Eagle v. Morgan*, Civ. No. 11-4303, 2011 U.S. Dist. LEXIS 147247 (E.D. Pa. Dec. 22, 2011)
- Address social media usage issues in a written policy

Create Document Return Policies

- Specify the return of both hard and soft copies
- Address the "Three Cs"
  - **C**o-mingling (of personal/work docs);
  - **C**ompliance (verifying)
  - **C**ost
- Have a standard protocol



Courtesy: manolaw.blogspot.com

Mobile Computing
Bring Your Own Device

- Have a written policy!
- Problems:
  - Monitoring use of devices
  - Protecting information from loss/theft
  - Prevent employee data theft
- Solutions:
  - Require installation of monitoring software
  - Require installation of remote-wipe software
  - Use software to prevent “pod slurping”

Mobile Computing
Bring Your Own Device

- Hacked phones can be used as listening and recording devices
- Prohibit employees from carrying smart phones and other devices with recorders into important business meetings



Image: Stefan Rousseau/PA Wire

Mobile Computing "Workshifting"

- Mobile computing and work shifting heighten ability of employees to obtain and hide employer documents
  - "Cloud" Computing
  - Personal hardware
- Employment contracts should address these topics



Courtesy: wombletradesecrets.blogspot.com

Protecting Good Will

- Clear & Consistent expectations regarding employee and ex-employee communications
  - Confidentiality
  - Non-disparagement
  - Social Media
- Review NLRB Reports on Social Media Usage
  - http://www.nlrb.gov/node/5078



Courtesy: www.stoelrivesworldofemployment.com

Employee Training

- Train IT staff on basic tasks:
  - Imaging devices
  - Preservation
  - Data recovery
- Chain of Custody (Procedures & Forms)
- Involve IT in terminations

Managing Termination

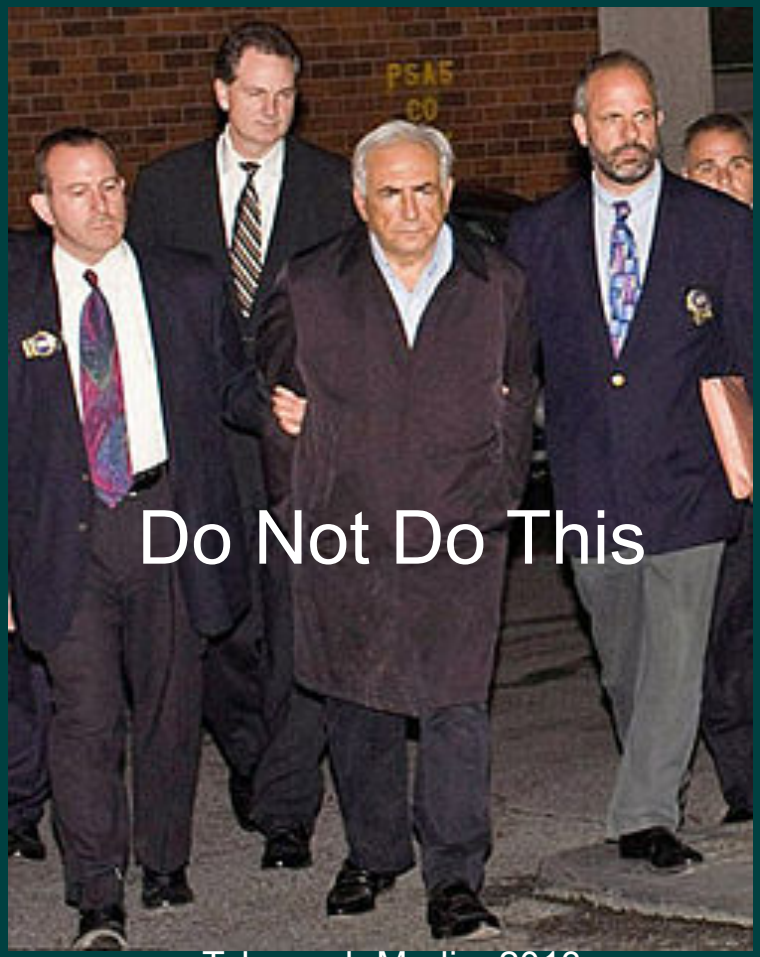


Termination Checklist

- Disable access to digital systems, devices, & accounts
- Retrieve access cards, keys, and badges
- Advise security that the employee is not to be permitted on the premises

Termination Checklist

- Secure the employee's laptop, desktop, and Company-issued devices
- Secure the employee's office/cubicle
- Arrange for the employee to remove personal possessions, under careful supervision, with **as little embarrassment as possible**



Telegraph Media, 2013

Exit Interview

- Incentivize departing employees to participate in exit interviews
- Have a well thought out checklist:
  - Return of documents
  - Return of other property
  - Discuss employee's continuing obligations
  - Retrieval of employee's property from his/her office

Exit Interview

- Key employee obligations:
  - Statutory (CFAA, Trade Secrets)
  - Contractual (Restrictive Covenants, Non-Disparagement, Confidentiality)
  - Common Law (Fiduciary Duties)
  - Consequences (Clawback)

Exit Interview

- Involve an IT professional in planning and executing this meeting
- If the exit interview or employee behavior evinces “red flags”, consider preemptively conducting a forensic examination of the employee’s electronic device(s)

Forensic Examinations



- Look for signs of:
  - USB Connections
  - Printer Usage
  - Scanned Documents
  - E-mailed documents
  - Read/reviewed documents
  - Uploaded documents
  - Phone records
  - Access to personal accounts over the internet
- Handle this examination with care to avoid privileged and private information
- This investigation may be instrumental in discovering evidence of document theft, collusion with new employer, and/or collusion with other employees

First Communication With Departing Employee's Attorney

- Remind the attorney of his/her client's obligations
  - Contractual (e.g. Return of documents, return of property, non-compete obligations, etc.)
  - Statutory (e.g. the CFAA, state computer use statutes, state Trade Secrets statutes, etc.)
  - Common Law (e.g. fiduciary duties)

First Communication With Departing Employee's Attorney

- Signal willingness to negotiate a reasonable protocol regarding the return of documents
- Discuss how personal information can be segregated from company owned information

First Communication With Departing Employee's Attorney

- Remind the attorney of his/her client's preservation obligations
- Identify the devices and/or information to be preserved (e.g. personal laptop, text messages, audio/video recordings, e-mail, web browser history, etc.)

Navigating the Ethical Minefield

- Notify employees that the Company can access all information stored on its servers
- Nevertheless, avoid accessing:
  - Attorney-client privileged material
  - Private Medical information
  - Private financial information





Navigating the Ethical Minefield

- Ethical implications of encouraging, aiding, and/or abetting document theft
- Ethical issues if counsel takes possession of stolen documents

Indemnification Clauses

- Review indemnification obligations carefully prior to termination
- Determine if the Company is arguably required to advance fees and costs to a departing executive in the event that the Company asserts claims against that executive, either under contract or under law (e.g. § 18-108 of the Delaware Limited Liability Company Act)
- If so, can the Company contractually or legally exclude such claims from its indemnification obligations

Additional Resources

- Dan Blake, Five Mistakes to Avoid in Drafting Non-Compete and Non-Solicitation Agreements, EPLI Risk, May 22, 2013, http://eplirisk.com/five-mistakes-to-avoid-in-drafting-non-compete-agreements/
- Harry Jones, Recent Study Reveals Troubling Amount of Employee Misuse and Theft of Company Data, Unfair Competition & Trade Secrets Counsel, Mar. 19, 2013, http://www.unfaircompetitiontradesecretscounsel.com/conversion/recent-study-reveals-troubling-amount-of-employee-misuse-and-theft-of-company-data/
- Kenneth J. Vanko, When a Restriction on Soliciting "Prospective" Customers is Unreasonable (and How to Fix It), Legal Developments in Non-Competition Agreements, Apr. 25, 2013, http://www.non-competes.com/2013/04/when-restriction-on-soliciting.html
- Ron Williams, Protecting Your Crown Jewels: Preventing Against and Responding to Intellectual Property Theft, Smart Business, June 1, 2011, http://www.sbnonline.com/2011/06/protecting-your-crown-jewels-preventing-against-and-responding-to-intellectual-property-theft/