Monday, October 1, 2012
11:00 AM - 12:30 PM

901 – Ethics and IP Theft

John Bates
Contract Negotiations Manager
U.S. Cellular Corporation

Joel Bush
Partner
Kilpatrick Townsend & Stockton LLP

Larisa Lacis
General Counsel
BTG Systems, Inc.

Ronald Potempa
Associate General Counsel
Infor Global Solutions, Inc.

Faculty Biographies

John Bates

John G. Bates is a contract negotiations manager within U.S. Cellular's IT strategic sourcing and vendor management group in Chicago, IL. His responsibilities include negotiation, drafting, and approval of large scale IT infrastructure agreements including professional services, software licensing, hardware/appliance acquisition, maintenance/support, outsourcing, and training.

Prior to working with U.S. Cellular, Mr. Bates served as in-house counsel and a business leader in a variety of technology industries including software development, electronic auditing, eCommerce, music licensing, manufacturing, and consumer electronics. A substantial portion of his career has focused on entrepreneurial technology companies involving a wide variety of legal areas including privacy, distribution, employment, manufacturing, international import/export, intellectual property, local taxation, and data privacy/security compliance.

Mr. Bates participates in several ACC activities including: secretary of the Intellectual Property Committee, ACC's Chicago Chapter liaison for the IT, Privacy & eCommerce Committee, member of International Legal Affairs Committee, and IP leader for the ACC's Chicago Chapter of the StreetLaw program.

Mr. Bates received a BA from the University of Illinois at Urbana-Champaign and JD from Illinois Institute of Technology, Chicago-Kent College of Law.

Joel Bush

Joel Bush is a partner at Kilpatrick Townsend & Stockton LLP in Atlanta, GA. He concentrates his practice in the area of complex commercial litigation, with particular emphasis in information technology and software disputes, misappropriation of trade secrets, business torts, restrictive covenant, and technology license disputes. Mr. Bush has litigated disputes arising out of computer hardware installations, software implementations, network design projects, and other technology infrastructure projects.

Mr. Bush regularly represents software and technology companies in claims based on a fraud, breach of contract, and negligence arising out of implementation problems, network design issues, software performance, and system compatibility problems. He has represented employers and employees in disputes arising out of restrictive covenant agreements. Mr. Bush routinely litigates trade secret disputes and he has particular experience in trade secret claims arising out of software development and software licensing. Mr. Bush also represents commercial parties in contract, indemnity, and related claims. He has appeared in federal and state courts and is also experienced in arbitration.

Mr. Bush has been recognized as a Georgia "Super Lawyer" in general litigation by SuperLawyers magazine and is AV(R) rated by Martindale-Hubbell.

Mr. Bush received a BA from Emory University and is a graduate of the University of Virginia School of Law.

Larisa Lacis

Larisa Lacis is vice president, life sciences, and general counsel at BTG Systems, Inc. (BTG), an IT services provider. Her responsibilities include managing all legal aspects of the business, along with business development activities related to the life sciences industry.

Prior to joining BTG, Ms. Lacis was general counsel and intellectual property counsel at NeoPharm, Inc., which later merged with Insys Therapeutics, Inc. At NeoPharm, Ms. Lacis managed all legal aspects of the business, with a primary focus on all intellectual property and contract matters. Prior to working as in-house counsel, Ms. Lacis practiced all aspects of patent and trademark prosecution and litigation in private practice in both Chicago and Los Angeles.

She currently serves on the board of Women in Bio, Chicago Chapter and participated in the ACC's Chicago's Street Law program this past year.

Ms. Lacis received a BS in biology from the University of Michigan in Ann Arbor and a JD from DePaul University in Chicago.

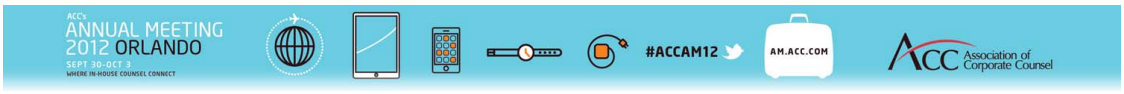
Ronald Potempa

Ronald E. Potempa is an associate general counsel at Infor Global Solutions, a global ERP software company located in the Chicago office. He is responsible for drafting, reviewing and negotiating all types of software agreements, including but not limited to: licensing, support, consulting, outsourcing, hosting, partnering, teaming, subcontracting and non-disclosure documents. He advises all levels of management from individual account executives through senior level vice- presidents. License compliance matters, settlement of disputes, and management of outside counsel are his other key responsibilities.

Prior to joining Infor, Mr. Potempa has worked as an in-house counsel for SSA Global, Sun Microsystems, Unisys, and Digital Equipment Corporation. He was responsible for providing legal counsel in a variety of substantive legal areas relating to hardware and software contracts, as well as areas such as employment disputes, purchasing activities, and leasing of office space.

He serves on the ACC's Chicago Chapter board of directors, and chairs the Diversity and Community Outreach Committee, which covers the Minority Law Student Internship Program, Street Law, and the Pro Bono activities. He is a Navy veteran and former member of the Navy Judge Advocate General Corps.

Mr. Potempa received his bachelor of business degree from Western Illinois University and his law degree from Loyola University of Chicago Law School.



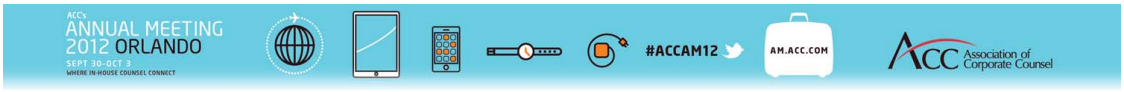
901 - Ethics and IP Theft

John Bates
Contract Negotiations Manager
U.S. Cellular Corporation

Larisa Lacis
General Counsel
BTG System, Inc.

Joel Bush
Partner
Kilpatrick Townsend & Stockton LLP

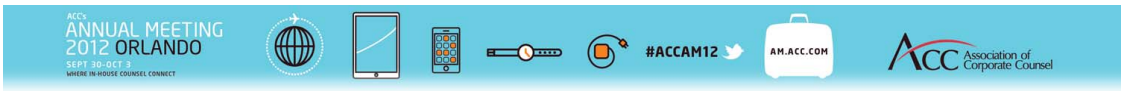
Ron Potempa
Associate General Counsel
Infor Global Solutions, Inc.



Overview

- Introduction to Trade Secrets & IP Theft
- IP Licensing & Protections
- Utilizing IT Solutions to Protect IP
- Special Considerations for Pharmaceutical, Medical, and Scientific Industries
- Identifying IP Theft

2



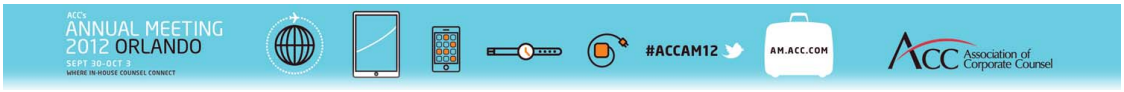
Trade Secrets and Theft of IP

2009 survey by Ponemon Institute (research group in Arizona) based on interviews of roughly 1,000 individuals who were laid off, fired, or changed jobs:

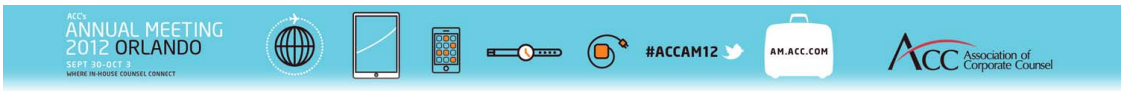
- 53% downloaded information to CD or DVD
- 59% steal confidential information from employer
- 42% downloaded information to USB drive
- 38% sent attachments to personal e-mail account

*82% said their employers did not conduct a review of their paper or electronic documents in conjunction with their departure!

3



Uniform Trade Secret Act



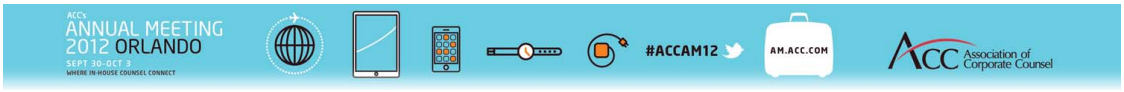
Trade Secrets

Trade Secrets are creatures of state law.

Uniform Trade Secrets Act (UTSA):

- Adopted in 47 states and District of Columbia
- New Jersey statute adopted on January 9, 2012
- Each state free to modify; there are variations even among states that have adopted UTSA
- Massachusetts – statute of its own based on common law
- New York and Texas – follow common law

5



Trade Secrets Under the UTSA

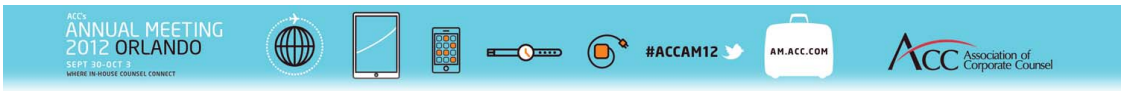
The UTSA defines a trade secret as "information, including a formula, pattern, compilation, program, device, method, technique, or process" that:

(i) derives independent **ECONOMIC VALUE**;

(ii) from **NOT BEING GENERALLY KNOWN** to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and

(iii) is the subject of efforts that are reasonable under the circumstances **TO MAINTAIN ITS SECRECY**.

6

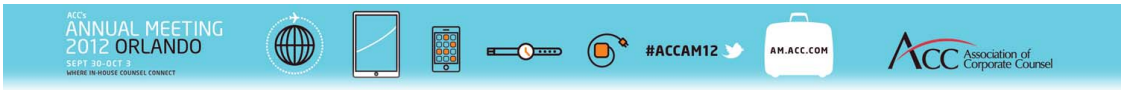


Variations Under the UTSA

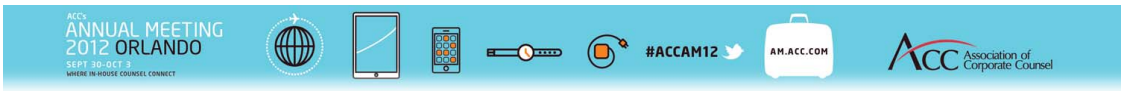
Variations to this standard definition across the states that have adopted the UTSA:

- Statute of limitations
  - 2 years (Alabama)
  - 3 years (most common)
  - 5 years (Georgia, Illinois, Missouri)
- Different rules regarding whether plaintiff must identify its trade secrets in pleading
  - California requires identification of trade secrets before discovery is allowed;
  - New York has been reluctant to impose this requirement

7



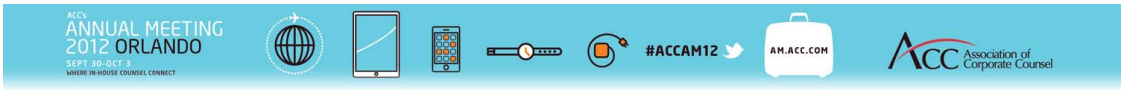
Computer Fraud and Abuse Act
18 U.S.C. § 1030 (1984)



Trade Secrets and Computer Fraud and Abuse Act

- Provides private cause of action against any individual who accesses "computer systems" to obtain information without authorization or exceeding authorized access
- Automatic federal jurisdiction
- No requirement to establish theft of trade secret or even that trade secrets were involved!
- If information is obtained improperly from a computer, CFAA increases litigation remedies
- Can be used to supplement trade secret claim
- Allows for injunctive relief and compensatory damages
- Attorneys' fees

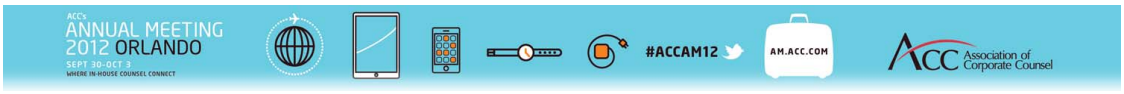
9



Computer Fraud and Abuse Act

- "Protected computer" is broadly defined to mean a computer "used in interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B).
  - Does not include:
    - Automatic typewriters
    - Handheld calculators
- In most contexts, violation must "cause[] loss aggregating at least $5,000 in value during any 1-year period to one or more individuals." 18 U.S.C. § 1030 (e)(8)(A)

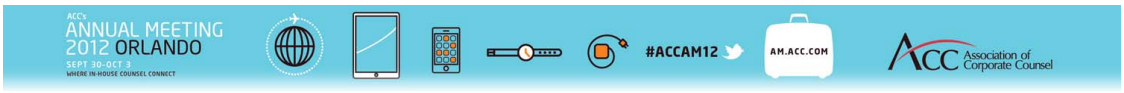
10



CFAA – Hotly Litigated Issue

Is a current employee acting with an improper purpose liable under the CFAA for accessing computer information that he or she otherwise had authorization to access?

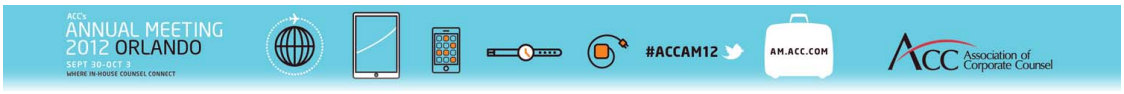
11



Application of the CFAA to Disloyal Employees

- Courts are split on whether "without authorization" or "exceeds authorized access" applies to the disloyal employee.
- The 11th Circuit has applied "exceeds authorized access" to find disloyal employees liable under the CFAA. *United States v. Rodriguez,* 628 F.3d 1258 (11th Cir. 2010).
- The 7th Circuit has found that disloyal employees are "without authorization" when accessing their employer's trade secrets. *Int'l. Airport Centers v. Citrin*, 440 F.3d 418 (7th Cir. 2006).

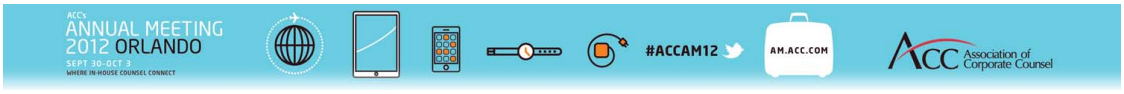
12



Application of the CFAA to Disloyal Employees

- Both the 1st and 5th Circuits have expressly found violations of the CFAA. *U.S. v. John*, 597 F.3d 263 (5th Cir. 2010); *EF Cultural Travel BV v. Explorica, Inc.,* 274 F.3d 577 (1st Cir. 2001).
- The 4th and 9th Circuits have rejected application of the CFAA to disloyal employees. *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009); *U.S. v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc); *WEC Carolina Energy Solutions, LLC v. Miller*, No. 11–1201, 2012 WL 3039213 (4th Cir. July 26, 2012).

13

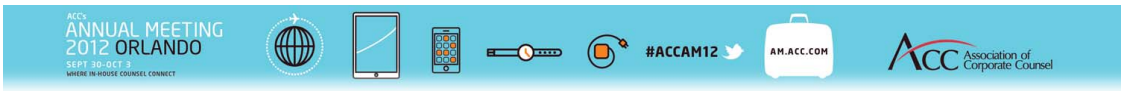


Preserving CFAA Claims

<u>Define "Authorized Access" In Employment Agreement</u>

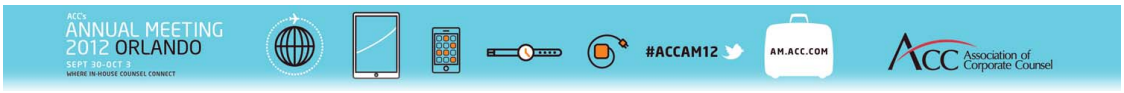
- Clearly defining an employee's scope of authorized access may allow an employer to maintain a CFAA claim.
- Include provision in confidentiality agreement that employee is not authorized to access company computers for "personal gain."
- Make clear the types of access that are "unauthorized."

14



Ethics Considerations:

Disclosure Restrictions in Trade Secret Litigation

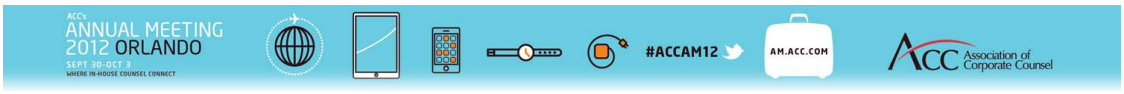


ABA Model Rules of Professional Conduct Rule 1.4 - Communication

A lawyer shall:

- "[K]eep the client reasonably informed about the status of the matter[.]"
- "[E]xplain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation."

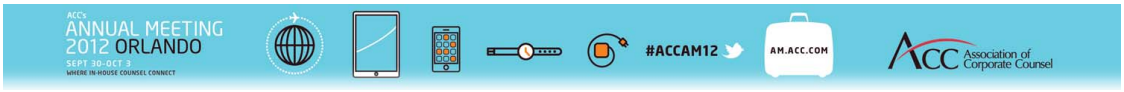
16



ABA Model Rules of Professional Conduct Rule 1.6 – Confidentiality of Information

"A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation[.]"

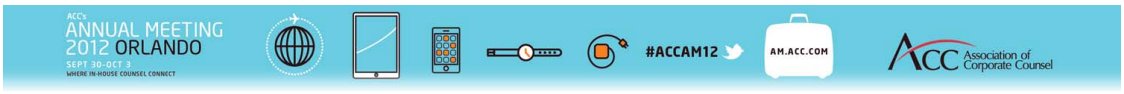
17



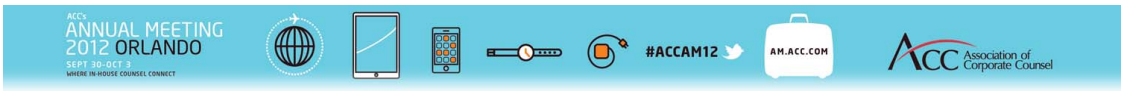
Protective Orders in Trade Secret Litigation

- Used to limit dissemination of "highly confidential" information to:
  - Outside Counsel
  - Court Personnel
- Outside counsel is obligated not to disclose the substance of "highly confidential" information learned during discovery, which is designated "outside counsel only."
- Courts have limited in-house counsel's access to "highly confidential" information where there is "an unacceptable risk of or opportunity for 'inadvertent disclosure' of confidential information." *Autotech Techs. Ltd. P'ship v. Automationdirect.com,* 237 F.R.D. 405 (N.D. Ill. 2006).

18



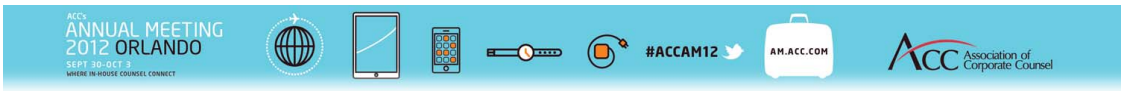
Trends in Trade Secret Litigation



Trends in Federal Trade Secret Litigation

- Federal trade secret litigation doubled from 1988 to 1995 and doubled again from 1995 to 2004. It is expected to double again by 2017.
- In over 85% of federal trade secret cases, the alleged misappropriator was someone that the trade secret owner knew.
- Trade secret owners are twice as likely to prevail on preliminary injunctive relief when they sue employees as compared to suits against business partners.
- Alleged misappropriators prevail at summary judgment in over 50% of federal cases.

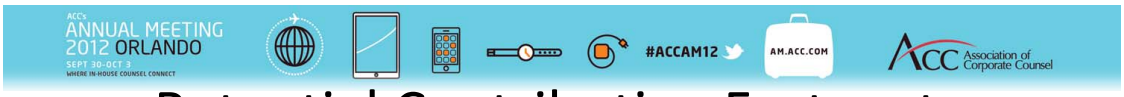
20



Trends in State Court Trade Secret Litigation

- In over 90% of state trade secret cases, the alleged misappropriator was an employee or business partner of the owner.
- Nearly half of all state trade secret cases occurred in 5 states: California, Texas, Ohio, New York, and Georgia.
- Reasonable measures were usually not satisfied if confidentiality agreements with employees and third parties were not in place.

21



Potential Contributing Factors to Increase in Trade Secret Theft

- Reductions in Workforce
- Dislocations Caused by Economic Conditions
- Cultural Shifts
  - Instant access to information
    - Dramatic increase of downloads of music and video
    - Decline in purchase of CDs and DVDs
    - Perception that information in cyberspace is “public”

22

Potential Value of Trade Secret Suits

Blockbuster Trade Secret Verdicts in 2011

- 2011 IP verdicts include the two largest-ever verdicts based on trade secret theft.
  - *E.I. DuPont de Nemours and Co. v. Kolon Industries, Inc.* (E.D. Va.): $920 Million
  - *Pacesetter Inc. v. Nervicon Co.* (Cal Super. Ct.): $2.3 Billion

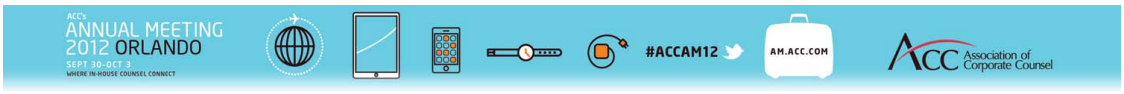
23

How Long Does a Trade Secret Last?

Forever . . .

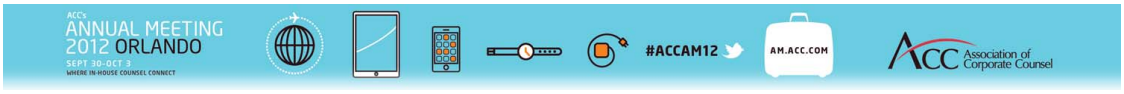
. . . until disclosed (how long can you keep a secret?), reverse engineered, or becomes part of the public domain.

24

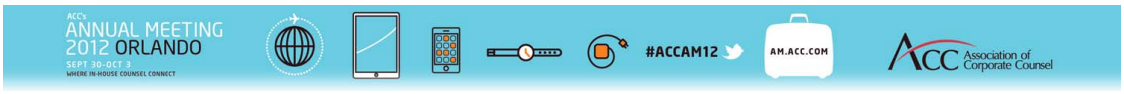


How Do You Keep a Trade Secret?

25



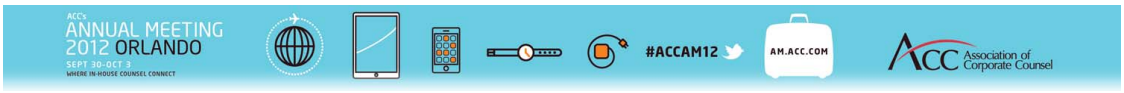
Enterprise Policies & Strategies to Protect Trade Secrets



Enterprise-Wide Strategies

- Strategies to protect trade secrets should include the entire enterprise
  - IT
  - Human Resources
  - Operations
  - Security
- Requires cooperation and coordination of multiple departments with varying expertise

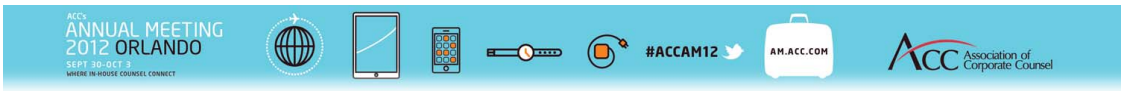
27



Enterprise-Wide Strategies

- New employee and recurring, periodic employee training about:
  - Existence of trade secrets
  - Protocols for protection of trade secrets
- Protection of trade secrets and IP through IT software solutions

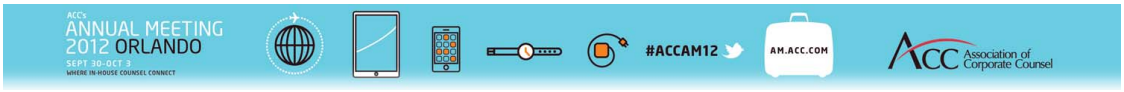
28



Protecting Trade Secrets

- Identify most valuable confidential information and control access
- Require confidentiality and non-disclosure commitments from employees
- Insist that customers and potential customers execute non-disclosure agreements
- Distribute information on a "need to know basis" and use "confidential designations"
- Confidentiality/non-disclosure policy, consider inclusion in employee handbook; separate policy; or free-standing agreement
- Establish protective measures that (1) are reasonable; (2) will be followed; (3) are sufficient to create a deterrent; and (4) will withstand scrutiny in litigation
- Conduct recurring employee training on established policies

29

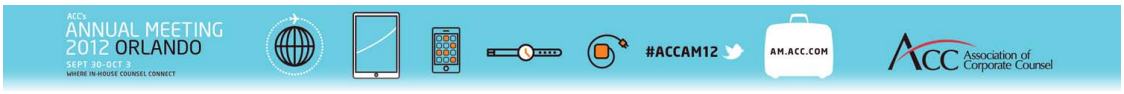


Protecting Trade Secrets When Employees Depart

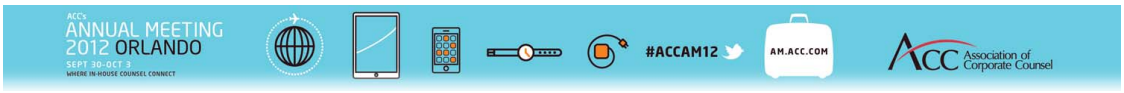
Conduct Exit Interviews

- Include review of confidential information that cannot be taken
- Remind employee of confidentiality agreements previously executed and explain that the obligations are ongoing
- Use a checklist!
  - "Do you have any company documents or materials at home?"
  - "Have you returned all flash drives that contain company information?"
  - "Have you made any copies by scanning or taking digital pictures of any company materials?"
- If doubtful, consider requesting the employee to sign affidavit or certification

30

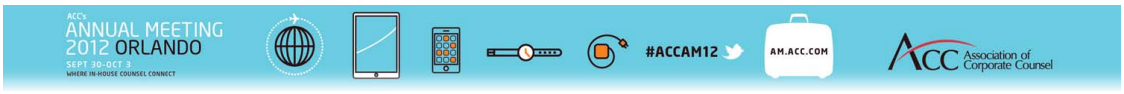


IP Licensing & Protections



IP Licensing - Introduction

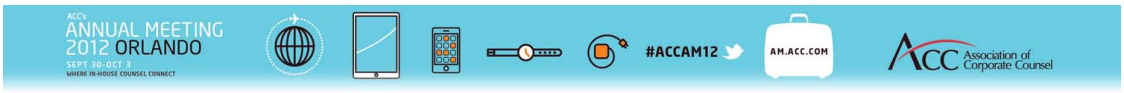
- Licensing Types
- Concurrent and Named Users
- Tier-Based CPU or Server
- Enterprise



Licensing Restrictions

- Perpetual
- Term
- Personal
- Non-Transferable
- Subsidiary or Affiliate Use
- Third Party Access (Service Provider)

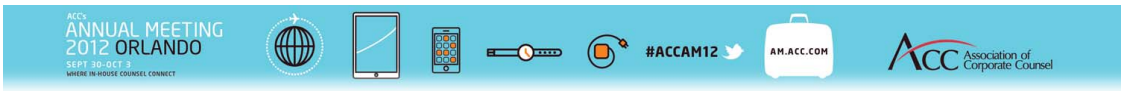
33



Right to Audit Clause

- Contract Provision – Yes or No
- Once Per Year Unless for Cause
- Notice Prior to Audit – 30 Days
- Purpose – Compliance with License Terms
- No Disruption to Customer's Business
- Performed at Licensor's Cost

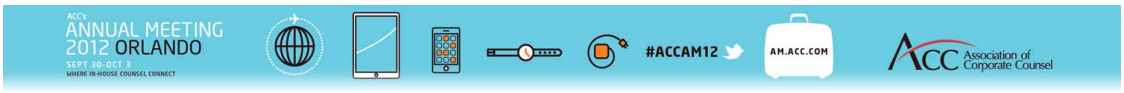
34



Audit Tools

- Software Tool That Can Extract Software Access and Usage
- Questionnaire
- Telephone Contact
- On-Site Visit

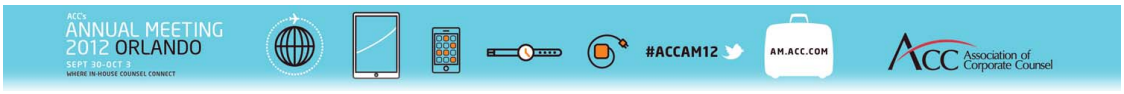
35



Examples of Audit Findings

- Software Running on CPU or Server That Was Not Designated in Agreement
- Excessive User Counts
- Third Party Access (Service Provider Accessing Software)
- Acquisition / Merger / Transfer / Assignment / Interim Processing
- Name Change

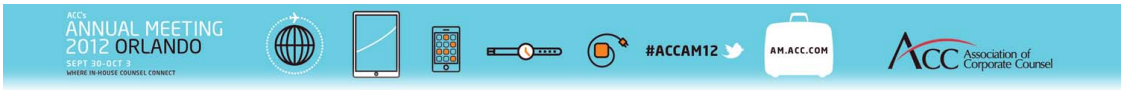
36



Tools & "Built-In" Protections

- Some Software is "Key Protected"
- Keys for CPU/Server Based Licensing and Access to Support
- Keys for User Count Restrictions
- Other Contractual Restraints
- Establish and empower software portfolio department responsible for recurring internal audits
- Consider software audit solutions that "scan" entire enterprise and generate reports about software, versions, locations, and usage

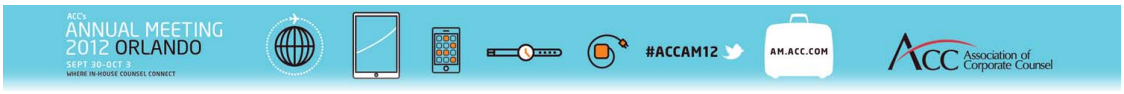
37



License Compliance

- Separate and Apart from Sales Function
- Contract Review by Pre-Audit Analysts
- Information Forwarded to Audit Coordinator
- Audit Coordinator is First Customer Contact
- Information Gathered Through Questionnaire or Software Audit Tool
- License Manager Shares Audit Results with Customer
- Discussions Regarding Bringing Software Use Into Compliance with Agreement

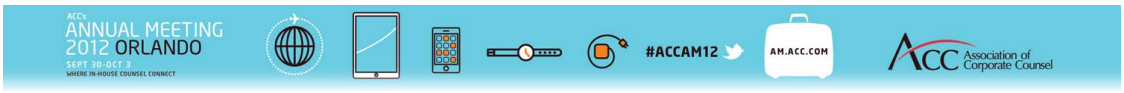
38



General Advice for Software Licenses

- Review License Grant Section of Current Software License Agreements
- Compare Actual Use with What is Authorized Under the Software License Agreement
- Avoid Pressure of Audit
- Build a Review Process of All Software Contracts
- Be Proactive

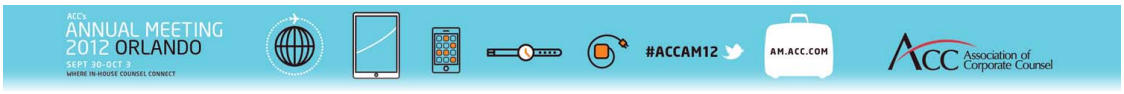
39



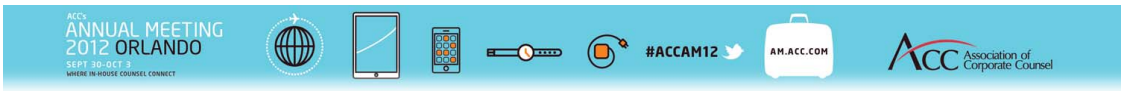
Summary

- Compliance is the Key
- Procrastination is Not an Option
- Educate All Employees
- Communicate Contractual Obligations to Those Who Have a Need to Know
- Comply with All Software License Requirements

40



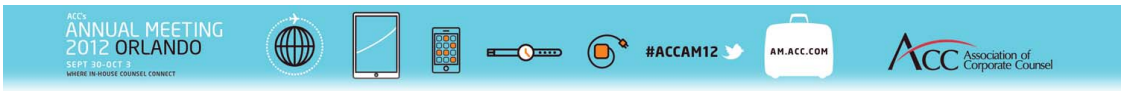
Utilizing IT Solutions to Protect IP



Introduction

- Create policies and procedures that prevent inadvertent mistakes
- Determined insider is difficult to stop and prevent from IP theft
- No organization is secure
- Following Best Practices for Data Loss Prevention ("DLP") will prevent trade secret/IP theft and data privacy breaches/thefts
- Must find creative solutions that balance security risks with allowing business to function
- Must create a cross-functional team to address holistic issue

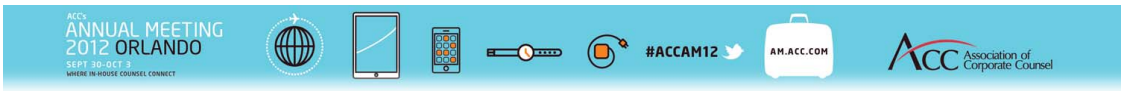
42



Two High Level Steps

- Step 1 - Control Access to Sensitive Data
  - Only give individuals access to the data that is required to perform their duties
- Step 2 - Background Checks
  - Comprehensive and reoccurring background checks
  - Eliminate problems before they begin

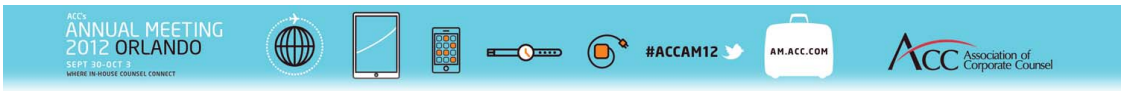
43



Role Based Access

- Create a Role Based Access Control ("RBAC") System
  - All data must be classified
  - All positions or levels of privilege must be established
  - Assign positions and individuals to data classifications

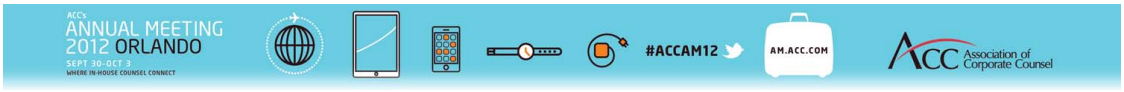
44



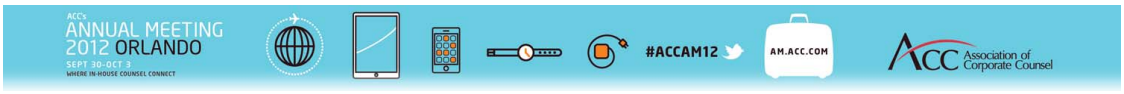
Education & Training

- Policies are not necessarily understood or intuitive to all employees
- Consider a pop up banner at the login screen that states that the employee will follow corporate policies. The pop up banner should include a click through acceptance of this statement so that they are reminded of the responsibilities of using the computer system.

45



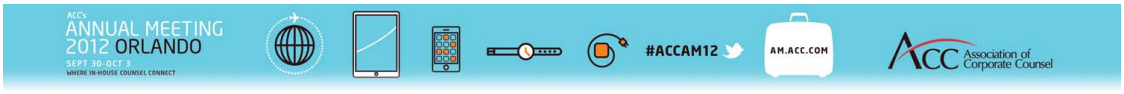
Network Management Tools



Log Management

- Consider software that analyzes and tracks who logins into entire network and audit file sharing
- Implement Network Access Control ("NAC") to present unapproved devices from attaching to the internal network
- Administrative Rights must be monitored and logged
  - These are the "keys to the kingdom"
- Limit file sharing programs to those who require data
- Database Access Management ("DAM") software that logs and monitors access and use of a corporate database
  - PCI compliance
  - Expensive, complex, and resource intensive
  - Documents theft, but will not prevent it
- Privilege Identity Management ("PIM")
  - Password vaulting
  - Creates an audit trail, notice, and allows control of sensitive passwords
  - Control root access to the entire corporate system
- Use 2 Factor Authentication (key fob, cell phone) when logging into the corporate system from a remote location

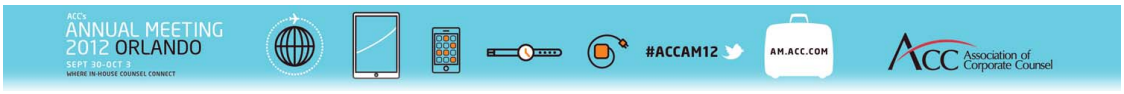
47



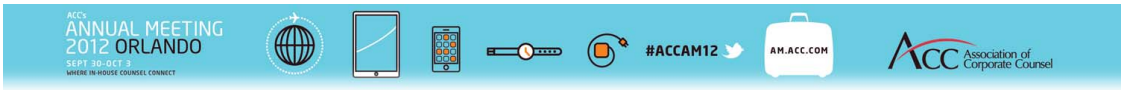
Vulnerability Scanning Solutions

- Can find applications on the network
- Used in combination with Application Whitelist programs that include all applications that can be used on a computer

48



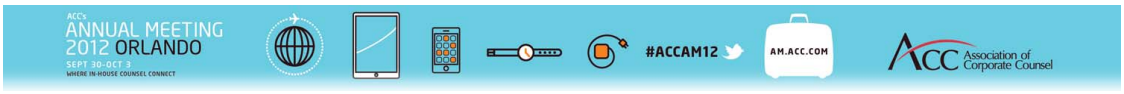
Limiting the Computer Client



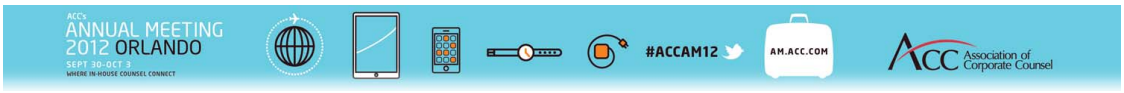
Limiting the Computer Client

- Elevate rights / remove administrative privileges for the user
  - Difficult if organization has allowed admin rights for users and then shifts to RBAC, change management and education must be utilized
  - Most cost-effective solution that an organization can implement
- Prevent USB drives
- Purchase corporate USB drives that are encrypted, password protected, and tracked
- Encrypt the hard drives of all computers (treat all computers the same)
- Encrypt the backups from the network
- Eliminate tapes and physical media backups (cd's, dvd's) because they get lost and can easily be stolen
- Require employees and consultants to use corporate computers in conjunction with NAC to control devices that can connect to your IP

50

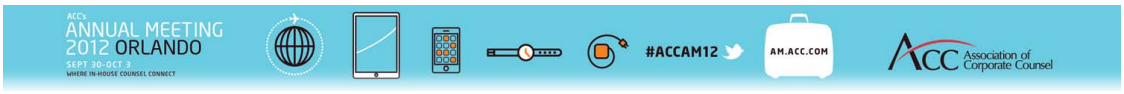


Controlling the Environment



Removing the Computer

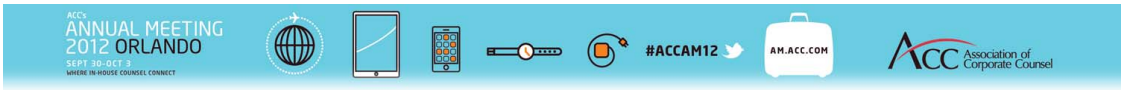
- Virtual Desktop Infrastructure ("VDI")
- Virtual Machine ("VM") is running on a server that is either internal or hosted offsite
- Virtual Private Network ("VPN") required for all devices (laptop, desktop, tablet) that connect to the corporate network
- Watch out for software licensing when using this solution!



Controlling the Web

- Utilize a proxy server that controls all outbound and inbound internet traffic
- Incorporate web filtering software that will prevent a remote login from a private computer to the corporate network (prevent Remote Desktop Access software programs)
- Include controls on Web Mail
- Prevent private drop box like cloud applications

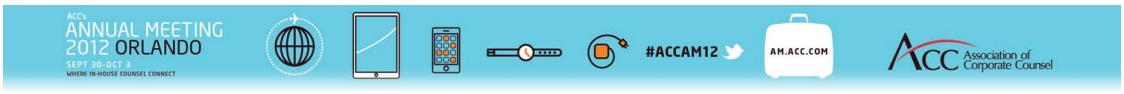
53



The Cloud

- Document storage
  - Control access and privileges
  - 2 factor logins
- Still requires same security personnel and procedures
- Sales Software as a Services (“SaaS”) has unique issues
  - Apply all the same access and privilege controls as physical storage
  - Difficult to prevent sales person from their own data
  - Directors have access to entire regions of sales information and contacts

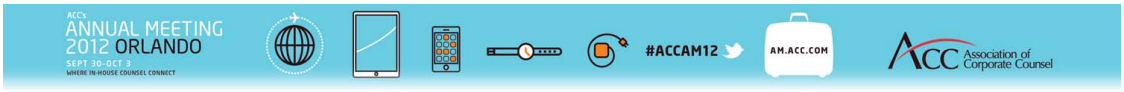
54



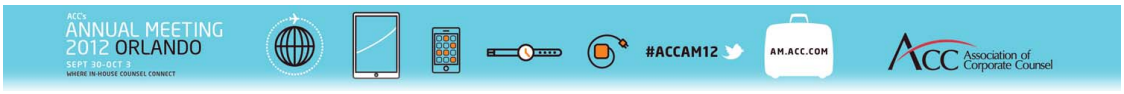
Mobile Devices

- Mobile Device Management Software / Bring Your Own Device ("BYOD")
  - Emerging area that presents new problems as phones and tablets are introduced
  - All data must be stored on VDI
  - Network Access Control software must be utilized to find jailbroken or rooted phones that have removed the accepted operating system - should alert to a policy violation

55



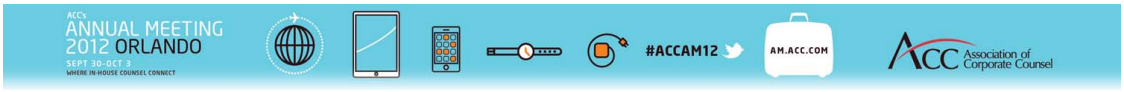
Special Considerations for Pharmaceutical, Medical and Other Scientific Industries



Special Considerations

- Inventions, technology, processes and data created in R&D labs are trade secrets until a patent application is filed or an article is published
- Most scientists and engineers are motivated to publish
  - Problem heightened if collaborate with universities or governments
- Trade Secrets v. patents
  - Methods of manufacturing technology often kept as trade secrets due to difficult enforcement of patents

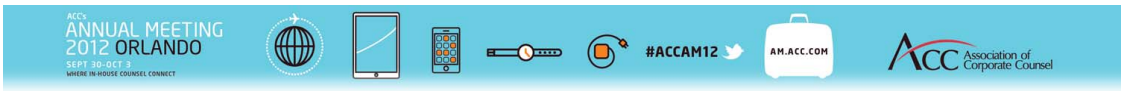
57



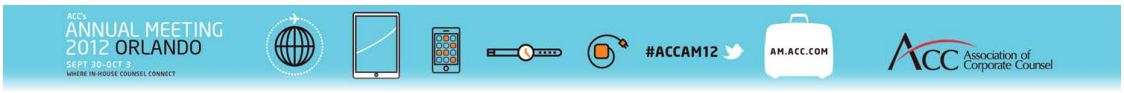
Special Considerations

- Quality control policies for lab notebooks
  - Distribution and return, limitations on physical use, restrictions on photocopying , etc.
  - work with Quality Assurance (QA) Department personnel
- Limit physical access to labs and include security procedures: sign in/out, fobs/key cards, etc., and only for qualified personnel.
  - Consider restrictions on digital cameras and phones
- Limit access to databases and documents with passwords, preclude or track use of USBs, email, printing, etc.
- Most lab functions are moving to electronic rather than paper-based (including lab notebooks), so IT security is key
- Trade secrets also include marketing and business development industry analytics, potential and current customer information and contract drafts and templates, etc.

58



Identifying IP Theft



How Does a Company Determine Whether It Is Stealing IP?

- Educate all employees
- Work with HR and conduct proper orientation interviews
- Have employees sign CDA/employee contracts with explanation of key provisions related to trade secrets
- Build a review process of all software contracts
- Communicate contractual obligations to those who have a need to know
- Comply with all software license requirements

60

How Does a Company Determine Whether Its IP Is Being Stolen?

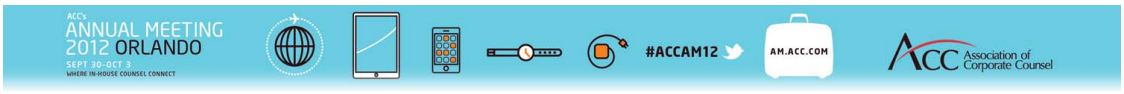
- Monitor ex-employee patent filings and article publications
  - Conduct regular FTO (freedom to operate) patent searches and analyses for company technologies
- If proof or hunch of misappropriation, send "cease and desist" letter

61

ACC's ANNUAL MEETING 2012 ORLANDO SEPT 30-OCT 3 WHERE IN-HOUSE COUNSEL CONNECT #ACCAM12 AM.ACC.COM ACC Association of Corporate Counsel

QUESTIONS?

62



Reference Materials

- Legal Requirements for Trade Secrets and Best Practices for Enforcement
  - Checklist for Guarding Against Loss of Trade Secrets
  - Sample Exit Interview Form
  - Sample Acknowledgement Regarding Trade Secrets and Proprietary Information for Incoming Employees
  - Sample Policy Language Concerning Use of Company Property and "No Personal Gain"
  - Sample Software Purchasing Guidelines & Checklist

63

901 - ETHICS & IP THEFT:

LEGAL REQUIREMENTS FOR TRADE SECRETS & BEST PRACTICES FOR ENFORCEMENT

John Bates
Joel Bush
Larisa Lacis
Ron Potempa

October 2012

TABLE OF CONTENTS

LEGAL REQUIREMENTS FOR TRADE SECRET PROTECTION

A trade secret is economically valuable, confidential information that is used in a company's business and that is not generally known to the public. Trade secrets are creatures of state law.

I. Trade Secret Law: The Uniform Trade Secret Act States vs. Common Law States

The Uniform Trade Secrets Act ("UTSA") has been adopted, with minor modifications, in 47 states. Most recently, New Jersey adopted the UTSA on January 9, 2012. In addition to their specific statutes, many states also rely upon the *Restatement (Third) of Unfair Competition* (1995) to determine the meaning of "trade secret." Three states have declined to adopt the UTSA; Texas and New York follow common law, while Massachusetts has adopted its own trade secret statute based on the common law.

A. The Uniform Trade Secret Act (UTSA) & Misappropriation

The UTSA defines a trade secret as "information, including a formula, pattern, compilation, program, device, method, technique, or process" that:

> (1) 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 disclosure or use; and
>
> (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

UTSA § 1(e).

Under the UTSA, misappropriation of a trade secret can occur in one of two ways[1]:

1. Improper Means Under the UTSA

Misappropriation may occur by the "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." UTSA § 1(c)(1).

The UTSA defines improper means to "include[] theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means." UTSA § 1(b).

[1] The UTSA provides a mechanism to obtain injunctive relief for "actual" or "threatened" trade secret misappropriation. UTSA § 2.

2. Disclosure Without Consent Under the UTSA

Misappropriation may occur through "disclosure or use of a trade secret of another without express or implied consent by a person" who:

(1) "used improper means to acquire knowledge of the trade secret," UTSA § 1(c)(2)(a),

(2) "before a material change of his [or her] position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake," UTSA § 1(c)(2)(c).

(3) "at the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was" either

(i) "derived from or through a person who had utilized improper means to acquire it,"

(ii) "acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use," or

(iii) "derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use." UTSA § 1(c)(2)(b).

The UTSA also includes provisions relating to injunctive relief (§2), damages (§3), and the award of attorneys' fees (§4).

B. The Common Law States: New York and Texas

A primary difference between the common law of trade secrets and the UTSA is the requirement of "continuous use." Under common law, in order to be a trade secret, information must be in "continuous use" by a company. This requirement eliminates a wide variety of information that would be considered a trade secret in a UTSA state but that may not be eligible for trade secret protection in a common law jurisdiction.

One particular category of trade secret that a "continuous use" requirement may disqualify is "negative know-how" or "negative trade secrets." This area of trade secret law has assumed heightened prominence, particularly as software and software development take a larger role in the economy. In essence, "negative know-how" is simply the knowledge of what path not to take to develop a product. For example, knowing which chemical formulations do not create a cancer-causing drug could be a trade secret under this doctrine. But, in a state requiring continuous use, this information would likely not be protected because the company is not actively using these failed formulations, and thus there is no "continuous use."

II. Representative Trade Secret Cases

A. Information Found to Constitute Trade Secrets

Generally, courts "define[] trade secrets broadly to include non-technical and financial data that derives economic value from not being generally known and is the subject of reasonable efforts to maintain its secrecy." *Camp Creek Hospitality Inns, Inc. v. Sheraton Franchising Corp.*, 139 F.3d 1396, 1410 (11th Cir. 1998).

1. Combinations of Components

- *Diamond Power Int'l v. Davidson*, 540 F. Supp. 2d 1322, 1337 (N.D. Ga. 2007) (party permitted to argue that although the "product was available in the public domain, information concerning its specialized components was not publicly available").

- *Essex Group, Inc. v. Southwire Co.*, 501 S.E.2d 501, 502-3 (Ga. 1998) (logistics system – "a warehouse organizational system with components extending from architectural layout features to customized equipment and modified computer software" – constituted a trade secret, even though it was composed of matters within the public domain, because it had been established that the "selection and arrangement of components and equipment" were unique to that system).

- *Tewari De-Ox Sys., Inc. v. Mountain States/Rosen, L.L.C.*, 637 F.3d 604, 613 (5th Cir. 2011) (noting that "a trade secret can exist in a combination of characteristics and components each of which, by itself, is in the public domain, but the unified process, design and operation of which in unique combination, affords a competitive advantage and is a protect[a]ble secret" and finding that combination of information publically available in a patent application with a proprietary process could be a protectable trade secret).

2. Computer Software

- *Elec. Data Sys. Corp. v. Heinemann*, 493 S.E.2d 132, 134 (Ga. 1997) (finding software designed as a "capital asset tracking system designed specifically for use by public utilities" and "a companion program for tax depreciation and tax asset value" constituted trade secrets).

- *Arminius Schleifmittel GmbH v. Design Indus., Inc.*, No. 1:CV00644, 2007 WL 534573 (M.D.N.C. Feb. 15, 2007) (holding that digital "library" containing customer's detailed specifications, CAD drawings, control programs, and photographs for sanding tools constituted a trade secret under North Carolina law).

- *Tradescape.com v. Shivaram*, 77 F. Supp. 2d 408, 419 (S.D.N.Y. 1999) (noting that computer software "indisputably is a subject of trade secret protection," and granting a preliminary injunction against a competitor who allegedly stole software source code).

3. "Tangible" Customer Lists

- *Morlife, Inc. v. Perry*, 66 Cal. Rptr. 2d 731 (1997) (holding that a compilation of names, addresses, and other customer data from business cards and from an employee's memory together constituted a trade secret because the employer had expended time and money in obtaining the data, the list was tailored to plaintiff's unique business, and the identity of the companies on the list was not generally known).

- *East v. Aqua Gaming, Inc.*, 805 So. 2d 932 (Fla. Dist. Ct. App. 2001) (finding that a list of viable potential customers was a trade secret when the plaintiff showed that the list was a product of great expense and effort).

- *Susqua Grp., Inc. v. Courtney*, No. 10-528(AD)(AKT), 2010 WL 3613855 (E.D.N.Y. Aug. 2, 2010) (holding that a customer list created through substantial effort and kept in confidence constituted a trade secret).

- *Paramount Tax & Accounting, LLC v. H & R Block E. Enters., Inc.*, 683 S.E.2d 141 (Ga. App. 2009) (holding that "the fact that certain individuals listed [in the telephone directory] have previously used [H & R] Block for tax preparation services is not [readily available]" and thus the client list could constitute a trade secret).

***But see*:**

- *Wachovia Ins. Servs., Inc. v. Fallon*, 682 S.E.2d 657, 663 (Ga. App. 2009) (concluding that "a public website titled 'freeERISA.com' contains all of the information" of the alleged trade secret and thus misappropriation claim failed as a matter of law).

- *Ris Paper Co. v. Wave Graphics, Inc.*, No. 040336, 2006 WL 2848672 (Mass. Super. Ct. Sept. 25, 2006) (finding that customer information could not be a trade secret because no physical list existed).

- *Leo Publ'ns, Inc. v. Reid*, 458 S.E.2d 651, 652 (Ga. 1995) (list of advertising clients compiled during employee's tenure – which included contact persons, telephone numbers, size, frequency and rates of advertising – was not a trade secret because it was "readily ascertainable by proper means" by, among other techniques, reading the newspaper and determining the identity of the advertisers).

4. Financial & Business Information

- *Camp Creek Hospitality Inns, Inc. v. Sheraton Franchise Corp.*, 139 F.3d 1396, 1410 (11th Cir. 1998) ("information concerning the Inn's occupancy levels, average daily rates, discounting policies, rate levels, long term contracts, marketing plans, and operating expenses" may constitute a trade secret under the Georgia Trade Secret Act).

- *Echostar Commc'n Corp. v. News Corp. Ltd.*, 180 F.R.D. 391 (D. Colo. 1998) (noting that revenue projections, price forecasts, pricing options, and competition strategies are ordinarily trade secrets).

- *Energex Enters., Inc. v. Anthony Doors, Inc.*, 250 F. Supp. 2d 1278 (D. Colo. 2003) (holding that methods of distribution and sales of a product can qualify as trade secrets)

- *B.U.S.A. Corp. v. Ecogloves, Inc.*, No. 05CIV. 988 (SCR), 2006 WL 3302841 (S.D.N.Y. Jan. 31, 2006) (holding that an employer's cost structures and bidding information were trade secrets when customers and most employees were not privy to the information).

- *Amedisys Holding, LLC v. Interim Healthcare of Atlanta, Inc.*, 793 F. Supp. 2d 1302, 1310-11 (N.D. Ga. 2011) (holding that business information regarding doctors' and hospitals' likelihood to refer patients for home health care services allowed "informed, fact-based decisions on where to focus . . . business solicitation efforts," which information "transforms an ordinary list of doctors and healthcare providers to a trade secret").

5. Scientific Data

- *Penalty Kick Mgmt. Ltd. v. Coca-Cola Co.*, 318 F.3d 1284 (11th Cir. 2003) (although certain aspects of the "Magic Windows" label were included in a patent application, and therefore rendered public, "many aspects of Magic Windows were unique," such as the unique production process, and therefore deserving of trade secret protection).

- *In re Continental General Tire*, 979 S.W.2d 609 (Tex. Sup. Ct. 1998) (holding that secret formula for skim stock used in manufacturing tires was a trade secret).

- *777388 Ontario Ltd. v. Lencore Acoustics Corp.*, 142 F. Supp. 2d 309 (E.D.N.Y. 2001) (holding that technical specifications and drawings related to sound-masking equipment were trade secrets).

- *Sensormatic Elecs. Corp. v. Tag Co. US, LLC*, 632 F. Supp. 2d 1147 (S.D. Fla. 2008) (holding that specifications for mechanical and magnetic features for labels attached to products were trade secrets).

- *Union Carbide Corp. v. Tarancon Corp.*, 742 F. Supp. 1565 (N.D. Ga. 1990) ("multiple dwell fluorination method," a special method of treating plastic containers, constituted a trade secret until the method was disclosed in a patent application).

PRACTICE POINTER

Conducting periodic trade secret audits will facilitate identifying trade secrets with particularity should the company find itself in the circumstance of bringing a claim for misappropriation.

B. Information Not Found to Constitute Trade Secrets

1. Intangible Lists of Customers or Suppliers

- *Zurich Depository Corp. v. Gilenson*, 121 A.D.2d 443 (N.Y. App. Div. 1986) (holding that mere recollection of customer information is not actionable).

- *Allen v. Hub Heaven, Inc.*, 484 S.E.2d 259, 263 (Ga. App. 1997) (cities that employer considered good candidates for new franchise location not a trade secret because "the general locations of unknown potential customers" cannot be considered trade secrets).

- *Ris Paper Co. v. Wave Graphics, Inc.*, No. 040336, 2006 WL 2848672 (Mass. Super. Ct. Sept. 25, 2006) (finding that customer information could not be a trade secret because no physical list existed).

- *Smith v. Mid-State Nurses, Inc.*, 403 S.E.2d 789 (Ga. 1991) (information in former employee's memory concerning: (1) nurses and facilities employer contracted with, including the reliability and availability of individual nurses; (2) the frequency certain facilities used agency nurses; and (3) the number of agency nurses the health facilities used, was not a trade secret because there were no efforts to protect the confidentiality of this information).

2. Particular Sales Methods

- *Capital Asset Research Corp. v. Finnegan*, 160 F.3d 683, 687 (11th Cir. 1998) (process by which business evaluated the amount to be bid on a tax deed, consisting of information available to the public, was "the same basic method by which any informed buyer would prepare to submit an intelligent bid at any auction," and thus could not constitute a trade secret).

- *Allen v. Hub Cap Heaven, Inc.*, 484 S.E.2d 259 (Ga. App. 1997) (allegedly "unique" technique of selling automotive trim pieces to body shops and car dealers by taking trucks full of unordered parts on regular sales routes, hoping to convince each dealer or body shop on the route to buy parts off the trucks, was used by other businesses in the United States and not subject to reasonable efforts to protect its secrecy, and therefore was not deserving of trade secret protection).

- *Electro Optical Indus., Inc. v. White*, 90 Cal. Rptr. 2d 680 (Cal. Ct. App.1999) (holding marketing plans and sales strategies were not trade secrets because they were matters of common knowledge).

3. General Employee Knowledge

- *Mirafi Inc. v. Murphy*, No. C-C-87-578M, 1989 WL 206491 (W.D.N.C. Oct. 23, 1989), *rev'd in part on other grounds by* 928 F.2d 410 (Fed. Cir. 1991) (holding that "[g]eneral

background knowledge and experience" acquired during the course of employment are not protectable as trade secrets).

- *Kitfield v. Henderson, Black & Greene*, 498 S.E.2d 537, 542 (Ga. App. 1998) ("[A]ny personal or subjective knowledge or other skills gained by Hendricks while working for Kitfield do not come under the Trade Secrets Act and their use may be prohibited only through restrictive covenants in an employment contract.").

- *Hogan Sys., Inc. v. Cybersource Int'l, Inc.*, 158 F.3d 319 (5th Cir. 1998) (holding that knowledge that could be obtained by means other than working for the employer was general knowledge and did not constitute a trade secret).

- *Unisource Worldwide, Inc. v. Carrara*, 244 F. Supp. 2d 977, 988 (C.D. Ill. 2003) (finding that "one who works for another cannot be compelled to erase from his mind all the general skills, knowledge, acquaintances and the over-all experience" of employment).

C. "Reasonable Efforts" to Maintain Secrecy

Whether a party seeking to enforce trade secret protections adopted reasonable efforts to keep the information secret "presents a question for the trier of fact." *Camp Creek Hospitality Inns, Inc. v. Sheraton Franchise Corp.*, 139 F.3d 1396, 1411 (11th Cir. 1998).

1. "Reasonable Efforts" Satisfied

- *Religious Tech. Ctr. v. Netcom On-Line Cmty. Servs., Inc.*, 923 F. Supp. 1231, 1253 (N.D. Cal. 1995) (holding that limiting access to information on a "need to know" basis, keeping documents under lock, and requiring employees to sign confidentiality agreements constitute reasonable efforts to maintain secrecy).

- *Stone v. Williams General Corp.*, 597 S.E.2d 456 (Ga. App. 2004), *rev'd on other grounds by* 614 S.E.2d 758 (Ga. 2005) (evidence that employer, in addition to restrictive covenant, restricted access to documents and instructed employees not to leave the building with them, was sufficient evidence to support the jury's verdict that reasonable efforts had been adopted).

- *Mangren Research & Development Corp. v. National Chemical Co.*, 87 F.3d 937 (7th Cir. 1996) (requiring employees to sign confidentiality agreements regarding a mold release formula, advising employees of the secrecy of the formula, and limiting access to the formula was sufficient to maintain secrecy).

PRACTICE POINTER

To protect valuable trade secrets, a company should consider the use of strict confidentiality agreements with all employees and other entities to which confidential information is disclosed, non-competition agreements with key employees, and restrict access to trade secrets and other confidential information on a "need to know basis."

2. "Reasonable Efforts" Not Undertaken

- *Diamond Power Int'l, Inc. v. Clyde Bergemann, Inc.*, 370 F. Supp. 2d 1339 (N.D. Ga. 2005) (denying manufacturer's request for preliminary injunction in part because manufacturer had sold product to the public and "made no real effort to maintain the confidentiality of the components at issue").

- *Geritrex Corp. v. Dermarite Indus., LLC*, 910 F. Supp. 955 (S.D.N.Y. 1996) (holding that an employer did not take reasonable steps to maintain secrecy when it did not require employees to sign confidentiality agreements and when it stored proprietary information in easily accessible areas).

- *Glaxo Inc. v. Novopharm Ltd.*, 931 F. Supp. 1280 (E.D.N.C. 1996) (when a company publicly disclosed a formula during a previous trial, its efforts to maintain secrecy were not reasonable).

- *Southwest Whey, Inc. v. Nutrition 101, Inc.*, 117 F. Supp. 2d 770 (C.D. Ill. 2000) (holding that limiting access to a secret process to one company, without requiring that company to sign a confidentiality agreement, did not constitute reasonable efforts to maintain secrecy).

- *Keane v. Fox TV Stations, Inc.*, 129 Fed. App'x 874 (5th Cir. 2005) (holding that reasonable efforts were not undertaken to maintain the secrecy of television show plans because the plaintiff mailed unsolicited letters detailing his ideas for American Idol to potential investors).

- *Roboserve, Ltd. v. Tom's Foods, Inc.*, 940 F.2d 1441, 1454-55 (11th Cir. 1991) (where product was sold on open market, trade secret law could not prevent the purchaser from dissecting the machine for purposes of reverse engineering; "[t]he sale destroyed any reasonable expectation of secrecy by placing the machines in the public domain").

D. Recent Cases

- *AvidAir Helicopter Supply, Inc. v. Rolls-Royce Corp.*, 663 F.3d 966 (8th Cir. 2011). AvidAir specialized in servicing helicopter engines built by Rolls-Royce. *Id.* at 969. AvidAir was told by the Federal Aviation Administration to stop servicing the engines because AvidAir did not have access to the correct procedures, which were outlined in a Distributor Overhaul Administration Letter from Rolls-Royce. *Id.* at 970. AvidAir obtained a copy of the letter without Rolls-Royce's permission, and Rolls-Royce sued AvidAir for misappropriation of a trade secret. *Id.*

  The Eighth Circuit acknowledged that the letter at issue was a compilation of both publicly-available and confidential information. *Id.* at 973. The Eighth Circuit found that the letter was a trade secret because it had independent economic value. *Id.* The Eighth Circuit attributed this value to the fact that the letter resulted from Rolls-Royce's own research and testing, and that all the information contained in the letter could not be

ascertained except through costly and difficult reverse-engineering. *Id.* Finally, the Eighth Circuit held that Rolls-Royce had engaged in reasonable efforts to maintain secrecy by never releasing the information in the letter without first requiring a confidentiality agreement. *Id.* at 974.

- *Amedisys Holding, LLC v. Interim Healthcare of Atlanta, Inc.*, 793 F. Supp. 2d 1302, (N.D. Ga. 2011). In this suit between two rival home healthcare and hospice service providers, the Court ruled that a company's collection, evaluation, and analysis of its customer information was a protectable trade secret. *Id.* at *1310.

  Amedisys brought suit against three former employees and their new employer alleging, among other things, misappropriation of trade secrets and violation of the Computer Fraud and Abuse Act ("CFAA"). Amedisys alleged that the employees had taken copies of Amedisys' Referral Logs and Workbook to their new employer, and that these documents constituted trade secrets. The Court found that, although the documents generally contained public information, such as the names of doctors and hospitals, they also contained Amedisys' internal observations regarding which doctors and hospitals were likely to refer patients to home health care, and how often, which information was not public. *Id.* at 1310-11. The Court found that this combination of public and proprietary information constituted a valuable trade secret. *Id.*

  The Court went on to find evidence sufficient to establish misappropriation against one of the three former employees based on that employee's e-mailing of copies of the Referral Logs and Workbooks from her work e-mail to her personal e-mail in the days before her separation. *Id.* at 1311. The Court also found that text messages between the former employee and her new employer indicated that the employee's intent was to use Amedisys' trade secrets at her new employer. Based on these facts, the Court, in granting a preliminary injunction, found a "likelihood of success on the merits" with respect not only to trade secret misappropriation, but also violations of the CFAA and vicarious liability against the new employer through a theory of respondeat superior. *Id.* at 1313, 1315-16. (Both the CFAA and the respondeat superior aspect of this decision are discussed in detail below.)

- *Fail-Safe, LLC v. A.O. Smith Corp.*, 674 F.3d 889 (7th Cir. 2012). Fail-Safe ("FS") and A.O. Smith ("AOS") entered a joint venture to develop a pump motor to prevent pool drains from trapping swimmers, and for which AOS would build a motor to FS's specifications. *Id.* at 891. The companies exchanged technology but could not agree on terms for the project. The two companies abandoned the project, but AOS later released two pumps that FS alleged incorporated FS trade secrets. *Id.*

  The Seventh Circuit held that FS had taken no precautions to safeguard the secrecy of the technology it shared with AOS, and it was therefore not a trade secret. *Id.* at 893. The court reasoned that FS willingly volunteered the technology without insisting upon confidentiality with AOS. *Id.* In fact, FS signed AOS's one-way confidentiality agreement but neglected similarly to protect its own disclosures. *Id.* The court also held

that AOS there was no implied duty of confidentiality in favor of FS and arising from the nature of the joint venture agreement. *Id.*

E. Emerging Issues In Trade Secret Litigation

1. "Negative Know How" and Negative Trade Secrets

In many research intensive industries, such as software and technology development, some of a company's most valuable information consists of knowing what path not to take to develop a product. In short, this application of trade secret law is very important in the computer field, because even a slight head start in the development of software or hardware can provide a significant competitive advantage. Courts in several jurisdictions have found that this "negative know how" or "negative information" may constitute a protectable trade secret.

- *Pincheira v. Allstate Ins. Co.*, 190 P.3d 322, 336, 144 N.M. 601, 615 (2008). In *Pincheira* the court found that trade secrets may include "business methods that [were] considered and rejected," because "competitors could use that information in developing their own processes."

- *Novell Inc. v. Timpanogos Research Group, Inc.*, 46 U.S.P.Q.2d 1197, 1217 (Utah Dist. Ct. 1998) ("'negative knowledge gives [former employees] a considerable head start or competitive advantage as they develop competing products for the market'").

- *On-Line Tech., Inc. v. Perkin-Elmer Corp.*, 253 F. Supp. 2d 313, 323 (D. Conn. 2003) (holding that "negative knowledge" is one form of "using" trade secrets, because "one may 'use' a trade secret in ways other than direct manufacture and marketing").

- *Foster-Miller, Inc. v. Babcock & Wilcox Canada*, 210 F.3d 1, 12 (Mass. 2000) (finding that negative information allowed competitor to develop product "more quickly than otherwise would have been possible because it started with" knowledge about competing company's unique "recipe" for small diameter high-pressure hose).

2. Public Availability and Disclosure on the Internet

In general, public disclosure will vitiate trade secret status. However, there are several cases for the proposition that, even if the constituent elements of a trade secret are publicly available, a unique combination or assembly of such information may nonetheless be subject to trade secret protection, assuming that the other requirements are satisfied.

- *Penalty Kick Mgmt. Ltd. v. Coca-Cola Co.*, 318 F.3d 1284 (11th Cir. 2003) is one of the leading cases as to whether the public availability of information potentially voids trade secret status. In *Penalty Kick*, the Court addressed the question of whether a concept that had previously been disclosed in another company's patent application could still be subject to trade secret protection. The company seeking protection, Penalty Kick

Management ("PKM"), had developed a method of printing a message on the inside of a beverage container label, which could be read once the container was emptied.

Coca-Cola, while conducting due diligence on PKM's method, discovered a previously filed patent application (issued to another company), which disclosed substantially the same concept for – printing a message on the inside of a beverage container label. When Coca-Cola proceeded to produce bottles using this method, PKM brought suit for trade secret misappropriation. The Court examined PKM's claim of trade secret status and found that PKM's method – nicknamed "Magic Window" – was a valid trade secret. *Id.* at 1291. The Court noted that although some elements were disclosed in a separate patent application, PKM's implementation was unique, utilizing ink, printing methods, and decoding methods that were different than those disclosed in the patent application. *Id.* The Court found that these elements were "not commonly known by or available to the public," and that trade secret protection could be maintained by PKM. (The court ultimately concluded, however, that Coca-Cola had not, in fact, misappropriated PKM's trade secrets.)

- *Tewari De-Ox Sys., Inc. v. Mountain States/Rosen, L.L.C.*, 637 F.3d 604 (5th Cir. 2011) addressed whether the combination of numerous pieces of publicly available information could nonetheless constitute a legally protectable trade secret. Tewari was the proprietor of a system for fresh-packing meat by removing all of the oxygen from inside the package. Tewari was contacted by Mountain States/Rosen ("MTSR") about applying MTSR's technique to fresh-package racks of lamb for MTSR. After a meeting at which Tewari disclosed its trade secrets – the method for removing all oxygen from inside the meat packaging – Tewari alleged that MTSR misappropriated Tewari's trade secrets. MTSR defended the suit by pointing out that information about each of Tewari's methods was publicly available and thus not subject to trade secret protection.

  The Fifth Circuit found that Tewari's combinations of various publicly available methods and techniques could be a protected trade secret. *Id.* at 613. The Fifth Circuit noted that "a trade secret can exist in a combination of characteristics and components each of which, by itself, is in the public domain, but the unified process, design and operation of which in unique combination, affords a competitive advantage and is a protect[a]ble secret." *Id.* The Fifth Circuit held that Tewari's "combinations of disclosed processes and technologies with other elements," created an issue of fact regarding whether the methods were protectable trade secrets, and therefore reversed the district court's summary judgment decision in favor of MTSR on that issue. *Id.* at 614.

Does trade secret material that has been posted on the Internet immediately and forever lose its trade secret status? Trade secret practitioners have generally assumed that it does. However, on August 18, 2011, a very significant ruling issued by Judge William H. Walls of the U.S. District Court for New Jersey concluded that various postings on the Internet in that case were not sufficient to waive trade secret protection.

- *SyncSort Inc. v. Innovative Routines, Int'l, Inc.*, No. CV-04-3623, 2011 WL 3651331 (D.N.J. Aug. 18, 2011) addressed whether brief but complete public disclosure of information on the internet voided trade secret protection of a company's proprietary software command language. The Court ultimately found that even complete public disclosure on the internet of the entirety of the claimed trade secret was not sufficient to void trade secret status because the internet disclosure was not widely known, was not widely used, and was quickly removed from the Internet. *Id.* at *14-15.

  SyncSort involved a dispute between two rival software companies who both developed and sold "data transformation" software. Each company had developed its own proprietary "coding language," which allowed their customers to write scripts to automate their routine data transformations. These two languages were incompatible with each other, making it extremely difficult for a customer to switch from one company's program to the competitor's program.

  Innovative Routines, International ("IRI") developed a program to translate scripts written for SyncSort's language into IRI's language for use with IRI's program. IRI developed their program using a version of SyncSort's Reference Guide, which defines the commands, syntax, and parameters of SyncSort's programming language, as well as utilizing trial and error to perfect their program. SyncSort's Reference Guide contains the entirety of what SyncSort considered their trade secret, and is only available to licensed customers who sign a confidentiality agreement.

  SyncSort sued IRI, alleging that IRI had misappropriated their trade secrets by developing the script translation program. IRI defended by alleging that SyncSort's language had lost trade secret status through various postings on the internet of both partial and complete versions of SyncSort's Reference Guide. The Court held that even though entire copies of the Reference Guide had been posted on the internet, once in Korea and once in Japan, the postings were "sufficiently obscure or transient or otherwise limited," and thus did not make the trade secret "generally known." *Id.* at *14. The Court found that because "the information was quickly removed upon discovery and there is no evidence that information became widely available or that competitors or other unauthorized persons accessed or even attempted to access the information," the Reference Guide's trade secret status was not necessarily lost. *Id.* at *15.

PRACTICE POINTER

Trade secrets should be stored in the "cloud" only after securing an express confidentiality agreement with the cloud computing service provider to assume legal responsibility for the security of the cloud.

3. *Respondeat Superior*: Employer Liability for Employee Misappropriation

In the last several years, several courts have addressed arguments that employers should be held liable for the misappropriation of trade secrets committed by their employees. The traditional example of holding a new employer liable is when the new employer knows of the employee's access to a competitor's trade secrets and actively encourages that employee to use that information in connection with the new employment relationship. Under this example, the employer could be directly liable based on the employer's actions.

However, since 2001, a few courts have expanded the scope of a new employer's potential liability under theories of respondeat superior and held employers responsible for acts committed entirely by their employees and without the employer's knowledge simply because the employee acted within the "scope of employment" when improperly using the trade secrets of another party. In one of the first cases to address this theory, a court in the Eastern District of Virginia held that an employer could be liable for an employee's misappropriation of trade secrets under a theory of respondeat superior because "[t]he employer reaps the benefit of the employee's misconduct and therefore should be liable for the harm that conduct causes." *Newport News Indus. v. Dynamic Testing, Inc.*, 130 F. Supp. 2d 745, 754 (E.D. Va. 2001).

In addition to Virginia, courts in Georgia, California, and Minnesota have recognized an employer's potential liability under a theory of respondeat superior, while only Indiana has expressly rejected the respondeat superior theory of liability in this context. See *Amedisys*, *supra*, 2011 WL 2182720 at *8-9 (N.D. Ga. June 3, 2011) (granting preliminary injunction in part based on "likelihood of success on the merits" of a trade secret claim and allegations of respondeat superior against a new employer); *Competitive Techs. v. Fujitsu Ltd.*, 286 F. Supp. 2d 1118, 1144-45 (N.D. Cal. 2003) (holding that "a principal may be liable for the tortious conduct of an agent, even if the principal has not authorized the conduct" and allowing trade secret claim to proceed against employer); *Hagen v. Burmeister & Assoc., Inc.*, 633 N.W.2d 497, 503 (Minn. 2001) (holding that respondeat superior was a valid theory of vicarious liability under the Uniform Trade Secret Act); but see *Infinity Prods., Inc. v. Quandt*, 810 N.E.2d 1028, 1034 (Ind. 2004) (holding that the theory of respondeat superior, as applied to trade secret misappropriation, was "displaced" by Indiana's trade secret act).

In *Amedisys*, Judge William Duffey found that although there was no direct evidence that the new employer had encouraged or assisted in its employee's misappropriation of a competitor's trade secrets, there was enough evidence to issue a preliminary injunction against the new employer because use of the wrongly appropriated trade secrets would "benefit" the new employer and "would be wrongful use within [the employee's] scope of employment" with the new employer. *Amedisys*, *supra*, 2011 WL 2182720 at *9 (N.D. Ga. June 3, 2011).

PRACTICE POINTER

To avoid potential liability under a theory of *respondeat superior*, employers should consider expressly defining the scope of employment NOT to include the unauthorized use of another party's trade secrets. Employment contracts should also expressly prohibit the disclosure or use of a former employer's trade secrets.

UTILIZING THE INEVITABLE DISCLOSURE DOCTRINE

The doctrine of "inevitable disclosure" evolved as a mechanism for an employer to seek to prohibit a former employee from post-employment activities when the proposed new employment would "inevitably disclose" the trade secrets of the former employer. In such a situation, an employer may seek to enjoin the disclosure of a trade secret (i.e., enjoin the new employment relationship for a limited time) based only on a theory of *threatened*, as opposed to *actual*, misappropriation. The theory underlying this doctrine is that an employee cannot "return" the knowledge acquired in her former position and, at least in certain situations, might necessarily call upon that knowledge in connection with the new employment relationship.

I. General Overview of Doctrine

The classic case of employee theft of tangible confidential information results in "actual" misappropriation, such as an employee walking out the door with a trade secret and turning it directly over to a competitor. In other situations, an employer may fear that misappropriation is "threatened" by the fact that a former employee has accepted a similar position with a competitor that renders trade secret disclosure "inevitable." To resolve these claims, courts must balance the former employer's trade secret rights against the employee's right to change employment positions freely.

The "inevitable disclosure" doctrine attempts to balance these competing interests. When the former employee's particularized knowledge and skills are inextricably tied to the former employer's trade secrets, employment with a direct competitor may pose a substantial risk that the trade secrets will be disclosed. Thus, even in the absence of deliberate theft of tangible confidential information, and notwithstanding the absence of any non-compete agreement, the former employer may pursue an injunction under an "inevitable disclosure" theory upon establishing: (1) the former employee possesses a valuable trade secret; (2) the employee has joined a competitor in a functionally equivalent position; and (3) in working for the new employer, the employee could not be expected ***not*** to use the trade secret. *See generally Milgrim on Trade Secrets* § 5.02 (discussing basic elements of inevitable disclosure doctrine).

II. A Jurisdictional Split

A majority of jurisdictions that have addressed the inevitable disclosure doctrine have adopted it, including Arkansas, Connecticut, Georgia, Illinois, Minnesota, Missouri, New Jersey, and North Carolina. However, the doctrine has been squarely rejected in California, Florida, and Virginia, primarily based on the theory that prohibiting future "threatened" misappropriation constitutes an unreasonable restraint on trade. *See, e.g., Whyte v. Schlage Lock Co.*, 101 Cal. App. 4th 1443 (Cal. Ct. App. 2002).

A. The Seventh Circuit's *PepsiCo* Opinion

The case widely viewed as outlining the inevitable disclosure doctrine is the Seventh Circuit's opinion in *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262 (7th Cir. 1995). In that case, PepsiCo sought to prohibit one of its general managers, who had access to high-level business plans and particularized marketing strategies, and who had signed a confidentiality agreement, from obtaining employment with Quaker Oats. At the time, PepsiCo manufactured a sports drink called "All-Sport," while Quaker Oats was known for "Gatorade."

The district court reasoned that "unless [the manager] possessed an uncanny ability to compartmentalize information," he would necessarily be required to make decisions regarding Gatorade by relying on PepsiCo's trade secrets, including specific "plans or processes" developed by PepsiCo and "disclosed to him while the employer-employee relationship existed, which are unknown to others in the industry and which give the employer an advantage over his competitors." *Id.* at 1269. The district court analogized that without some sort of injunction, "PepsiCo finds itself in the position of a coach, one of whose players have left, playbook in hand, to join the opposing team before the big game." *Id.* at 1270.

In holding that disclosure of PepsiCo's trade secrets was inevitable, the district court relied upon a number of factors, including: (1) the existence of a valuable trade secret; (2) exposure of the former employee to the trade secret; (3) direct and fierce competition between the former and current employers; (4) the degree of equivalency between the new position and the former position; and (5) lack of candor and credibility of the former employee. *Id.* at 1270-71.

The "lack of candor" factor appears to have greatly influenced the district court's decision. The PepsiCo manager, after accepting the Quaker Oats position, told his current employer that he had received an offer but he did *not* disclose at that time that he had, in fact, accepted the offer with PepsiCo's competitor. *Id.* at 1264. Further, and again without disclosing that he had accepted the offer at Quaker Oats, the PepsiCo manager asked whether PepsiCo approved his continued solicitations to PepsiCo customers, and PepsiCo said yes. *Id.* These examples of the manager's lack of candor led the district court to conclude that that the former PepsiCo manager "could not be trusted to act with the necessary sensitivity and good faith." *Id.* at 1270. While the district court granted injunctive relief, which injunction was upheld on appeal, the time period was narrow: the PepsiCo manager was enjoined from accepting the position at Quaker Oats for a period of only six months (from December 1994 through May 1995). *Id.* at 1272.

B. *Papermaster*: Apple v. IBM

In late 2008, Apple recruited and hired Mark Papermaster, one of IBM's top executives, an IBM employee for 26 years, and a widely recognized expert in IBM "power" architecture and microprocessor chip design. IBM sued Papermaster in the Southern District of New York for breach of contract and misappropriation of trade secrets based on a theory

of inevitable disclosure. Only a few months earlier, Apple had acquired a microchip design company in order to compete directly with IBM. *Papermaster v. Int'l Bus. Machines, Inc.*, No. 08-cv-9078, 2008 WL 4974508 (S.D.N.Y. Nov. 21, 2008). Concluding that Papermaster would inevitably use his experience at IBM to ensure that Apple's iPhones and iPods were fitted with the best available microprocessor technology, the Court issued an injunction preventing Mr. Papermaster from continuing his employment with Apple.

Notably absent was any evidence supporting the fifth *PepsiCo* factor, the candor and credibility, and lack of good faith of the employee. In fact, the Court found no evidence that Mr. Papermaster had been less than truthful or forthcoming about his intention to join Apple, stating that "the Court does not mean to suggest that Mr. Papermaster has intentionally acted dishonorably [and] . . . the Court has no evidence before it that Mr. Papermaster has disclosed any IBM trade secrets." *Id.* at *10.

However, Papermaster had executed a non-compete agreement in favor of IBM and in which Papermaster had acknowledged that IBM would suffer "irreparable harm" if he violated the non-compete agreement. According to the court, this "explicit provision in the agreement," in addition to "common sense," indicated that "IBM would be irreparably harmed by the disclosure of the important technical and proprietary information that Mr. Papermaster carries in his head." *Id.* at *9.

This case represents a broad reach of the inevitable disclosure doctrine, although the outcome may have been influenced by the high-level positions that were at issue and the media attention at the time to Apple's iPhone and iPod products.

C. *Bimbo Bakeries* and Thomas' English Muffins

In 2010, the Third Circuit issued a landmark decision on the inevitable disclosure doctrine. In *Bimbo Bakeries USA, Inc. v. Botticella*, 613 F.3d 102 (3d Cir. 2010), the Third Circuit upheld a preliminary injunction issued under Pennsylvania law to prevent a senior executive of Bimbo Bakeries from joining a competitor, Hostess. *Id.* at 105-106.

The executive in question, Botticella, was Bimbo Bakeries' vice president of operations for California, and had access to Bimbo Bakeries' trade secrets, including access to the Thomas' English Muffins recipe (which access was restricted to seven company employees). *Id.* When Botticella informed Bimbo Bakeries of his departure to Hostess, three months after secretly accepting the job, Bimbo Bakeries sued under an inevitable disclosure theory. *Id.* at 105. Botticella's employment agreement did not contain a non-competition clause restricting his post-Bimbo employment. *Id.*

The Third Circuit affirmed the district court's preliminary injunction in favor of Bimbo Bakeries, upholding the district court's reasoning that there was a "substantial likelihood, if not an inevitability, that [Botticella] will disclose or use Bimbo's trade secrets in the course of his employment with Hostess." *Id.* at 110. The Third Circuit did not go so far as to find that the disclosure would be "inevitable," but instead found that Bimbo needed only to prove that a "substantial threat of trade secret misappropriation" existed. *Id.* at 114.

Perhaps most helpful to Bimbo's claim was Botticella's suspicious behavior before leaving Bimbo, including "not disclosing to Bimbo his acceptance of a job offer from a direct competitor, remaining in a position to receive Bimbo's confidential information and, in fact, receiving such information after committing to the Hostess job, and copying Bimbo's trade secret information from his work laptop onto external storage devices." *Id.* at 118.

In other words, had Botticella been entirely candid and forthcoming with his actions after accepting the Hostess position, the outcome of the case might have been different. Like the decision in *PepsiCo*, the outcome in *Bimbo Bakeries* may have resulted from the lack of candor that Botticella exhibited toward his former employer.

THE COMPUTER FRAUD AND ABUSE ACT (CFAA)

The Computer Fraud and Abuse Act was originally enacted as a criminal "anti-hacking" statute in 1984 to protect government agencies and companies from improper access into their computer systems by "hackers." This federal criminal statute was amended in 1994 to add civil provisions. The explosion of the Internet and computer use in the private sector, coupled with the CFAA's relatively ambiguous language and private right of civil action, has led the CFAA to become an important tool in the arsenal for companies looking to protect their confidential information, and in effect allows companies to pursue trade-secret-like claims *without establishing the existence of a trade secret* in circumstances in which computer systems are accessed "without authorization."

Under the CFAA, a person who "intentionally accesses a protected computer without authorization or exceeds authorized access, and thereby obtains . . . information" has committed a crime. *See* 18 U.S.C. § 1030(a)(2)(C). A "protected computer" is simply any computer which "is used in or affecting interstate or foreign commerce" thus making the scope and reach of the statute almost limitless. *See* 18 U.S.C. § 1030(e)(2)(B). The civil provisions provide that "[a]ny person who suffers damage or loss . . . may maintain a civil action against the violator to obtain compensatory damages and injunctive relief." 18 U.S.C. § 1030(g). In order to maintain a civil action under the CFAA, a plaintiff must reach a threshold level of injury, the simplest of which is damage totaling over $5,000. *See* 18 U.S.C. § 1030(g) (referencing the damage requirement in 18 U.S.C. § 1030(c)(4)(A)(i)(I)).

Adding a CFAA claim to a trade secret complaint can be useful because it provides federal question jurisdiction and it allows employers to seek protection for information which might not be afforded trade secret status but is nonetheless confidential and proprietary.

I. Applying the CFAA to Disloyal Employees: "Exceeds Authorized Access" v. "Without Authorization"

Courts have wrestled with the extent to which the CFAA applies to actions taken by employees while still ostensibly working on the employer's behalf. *See generally Pacific Aerospace & Elecs., Inc. v. Taylor*, 295 F. Supp. 2d 1188, 1196-97 (E.D. Wash. 2003) (noting that employers "are increasingly taking advantage of the CFAA's civil remedies to sue employees and their new companies who seek a competitive edge through wrongful use

of information from the former employer's computer system."). "Since the beginning of 2008 alone, there have been at least 26 U.S. district court decisions in this area." Robert D. Brownstone, *Proper Parties to CFAA Claim: Split in Authority as to Whether a Defendant Can Be a Disloyal Employee Initially Granted Authorized Access to an Employer's Electronic Information Systems*, Data Sec. & Privacy Law: Combating Cyberthreats § 9:13.50 (2009). Because the federal district courts have taken varying approaches to this topic, it is important to be aware of both the potential causes of action and their limitations.

The primary CFAA section used in civil litigation, 18 U.S.C. § 1030(a)(2), provides a cause of action for two types of violations – (1) if an individual "exceeds authorized access" to a protected computer, or (2) if a person accesses a protected computer "without authorization." In a typical factual scenario in which an employer may consider using the CFAA, the disloyal employee has accessed company information for a use, personal or otherwise, that the company does not condone. This conduct may include an employee's downloading trade secrets to a personal computer to take to another company, or could be an employee accessing an internal company database in order to obtain consumer information for purposes of identity theft.

Courts have imposed liability under the CFAA under both of these fact patterns and under both the "without authorization" and "exceeds authorized access" theories of liability. Under the "without authorization" theory, an employee "loses" his or her authorization to access company systems upon committing a disloyal act. In contrast, under the "exceeds authorized access" theory, an employee retains his or her authority to access company systems but is not allowed to use or access the company information for an unauthorized purpose.

PRACTICE POINTER

In order to preserve flexibility for satisfying both the "without authorization" and "exceeds authorized access" theories of liability under the CFAA, companies should strictly prohibit the use of company computer resources for "personal gain," as well as maintain clear and specific policies governing use of and access to company computer systems by employees.

A. Cases Discussing "Without Authorization"

- *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2006). In the seminal case on the topic of access "without authorization," the defendant quit his employment and went into business for himself in competition with his former employer and in breach of his employment contract. Before returning his employer-issued laptop, the employee utilized a secure-erase program that erased his employer's data as well as data demonstrating his formation of a new business. The court held that the employee breached his duty of loyalty (by virtue of breach of his employment agreement) and therefore "terminated his agency relationship . . . and with it his authority to access the laptop, because the only basis of his authority had been that [agency] relationship." *Id.* at 420-21. Because his actions were a breach of loyalty to his employer, the employee

lost his rights of access, and was accordingly subject to liability under the CFAA under a theory of "without authorization."

- *ViChip Corp. v. Lee*, 438 F. Supp. 2d 1087 (N.D. Cal. 2006). In this case, the company brought various claims against its former CEO, including violation of the CFAA, claiming that the CEO stole confidential and proprietary information. The former CEO admitted that he deleted computer files, but argued that his actions were authorized because the deletion occurred while he was still an officer and director of the company. Again relying upon the Seventh Circuit's decision in *Citrin*, the *ViChip* court found this argument "unpersuasive." *Id.* at 1100. The court concluded that when the employee "decided – the night before his termination and *after* knowing that he was being asked to step down and give up his duties at ViChip – to delete all information from ViChip's server and his ViChip-issued computer, he . . . breached his duty of loyalty and terminated his agency relationship to the company." *Id.* Relying on *Citrin*, the court concluded that "[i]n doing so . . . he also terminated his authorization to access the files." *Id.* Thus, the employer was entitled to summary judgment on its claim that its former CEO was liable under the CFAA. The reasoning of this decision is likely overturned by *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012), discussed below.

- *Lasco Foods, Inc. v. Hall & Shaw Sales, Mrktg., & Consulting, LLC*, 600 F. Supp. 2d 1045 (E.D. Miss. 2009); *Lasco Foods, Inc. v. Hall & Shaw Sales, Mrktg., & Consulting, LLC*, No. 4:08CV01683 JCH, 2009 WL 3523986 (E.D. Mo. Oct. 26, 2009). Plaintiff Lasco Foods sued two former employees and the LLC that they formed subsequent to their employment with Lasco, alleging various causes of action, including violations of the CFAA. Defendants moved to dismiss the first amended complaint, arguing, *inter alia*, that Lasco had not sufficiently alleged a damage or a loss as required by the CFAA. *See* 600 F. Supp. 2d at 1051. In the first amended complaint, Lasco alleged that one of the defendants "deleted confidential and trade secret information" from Lasco's computer and "unlawfully copied or otherwise downloaded Lasco's Trade Secret Information for his own personal use and for the use of [the competing company] prior to his departure from Lasco and prior to deleting the Trade Secret Information from his Lasco computer and returning the computer to Lasco." *Id.* The court held that the allegations that defendants "deleted information are sufficient to allege 'damage,' as defined under [the] CFAA." *Id.* at 1052. The court also held that "the deletion of information, the cost of the forensic analysis and other remedial measures associated with retrieving and analyzing Defendants' computers constitute 'loss' under [the] CFAA." *Id.* Nevertheless, because Lasco "failed properly to allege 'without authorization," the court granted defendants' motion to dismiss. *Id.* at 1053.

  Lasco thereafter filed a second, and ultimately a third, amended complaint. Defendants again moved to dismiss, arguing again that Lasco failed adequately to allege that the former employees had accessed the information "without authorization." *See Lasco Foods, Inc. v. Hall & Shaw Sales, Mrktg., & Consulting, LLC*, No. 4:08CV01683 JCH, 2009 WL 3523986 (E.D. Mo. Oct. 26, 2009). Summarizing the pertinent case law – including *Citrin* – the court held that the defendants' alleged wrongful access of

confidential and trade secret information while they were still employed by Lasco stated a cause of action under the CFAA. *Id.* at *4. The court relied on Lasco's allegations that the defendants had authorization to access the information only in furtherance of the interests of *the employer*, and thus accessing the information to advance their *own* interests was unauthorized:

> Under the statute, the Restatement, and the reasoning of *Citrin* and other courts, Lasco sufficiently alleged that Hall and Shaw acted without authorization when they obtained Lasco's Information for their personal use and in contravention of their fiduciary duty to their employee, Lasco.

Id.

- *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009). The Ninth Circuit in *Brekka* affirmed a Nevada district court's grant of summary judgment in favor of the defendants on claimed violations of the CFAA under circumstances similar to those of *Citrin*. The court equated current employment with "authorized" access:

> Because Brekka was authorized to use LVRC's computers while he was employed at LVRC, he did not access a computer "without authorization" in violation of § 1030(a)(2) or § 1030(a)(4) when he emailed documents to himself and to his wife prior to leaving LVRC. Nor did emailing the documents "exceed authorized access," because Brekka was entitled to obtain the documents.

Id. at 1127. In so holding, the court rejected the analysis of *Citrin* on a number of grounds. In particular, the court concluded that "[t]he plain language of the statute . . . indicates that 'authorization' depends on actions taken by the employer. Nothing in the CFAA suggests that a defendant's liability for accessing a computer without authorization turns on whether the defendant breached a state law duty of loyalty to an employer." *Id.* at 1135. Rejecting *Citrin*'s interpretation, the court concluded that access is "without authorization" *only* when an employee has *no permission* to access computer systems for *any* purpose:

> a person uses a computer "without authorization" under §§ 1030(a)(2) and (4) when the person has not received permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway.

Id.

B. Cases Discussing "Exceed[ing] Authorized Access"

- *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010). On December 27, 2010 the Eleventh Circuit, in the *Rodriguez* case, held that an employee exceeded authorized access upon accessing company computer systems for an improper purpose. *Id*. at 1263. Roberto Rodriguez was a TeleService representative for the Social Security Administration ("SSA") where his duties included answering general questions about social security benefits. *Id.* at 1260. As part of his job, Rodriguez had access to databases containing sensitive personal information, including names, addresses, dates of birth, and social security numbers. *Id.* The SSA, which carefully monitors access to these databases, tracked Rodriguez's accessing the database for non-business reasons 17 times over the course of his employment. *Id.* For example, Rodriguez accessed the information of his ex-wife as well as a former roommate for non-business reasons. *Id.*

  The Government filed criminal charges against Rodriguez under the CFAA, alleging that he had "exceeded authorized access" by accessing the personal information of numerous individuals for non-business reasons. *Id.* Rodriguez, citing *Brekka*, argued that he could not be convicted under the CFAA because, by virtue of his employment, he had "authorized access" to the databases. *Id.* at 1263. The Eleventh Circuit rejected Rodriguez' arguments and distinguished *Brekka*, holding that "the [SSA] told Rodriguez that he was not authorized to obtain personal business information for non-business reasons" and therefore Rodriguez "*exceeded his authorized access* and violated the [CFAA] when he obtained personal information for a non-business reason." *Id.* (emphasis added).

- *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc). On April 10, 2012, the Ninth Circuit issued an *en banc* decision in *Nosal*, finding that the phrase "exceeds authorized access" was not meant to criminalize an employee exceeding his employer's computer use policies by "g-chatting with friends, playing games, shopping or watching sports highlights" on his work computer, but rather was intended to criminalize "hacking" into an employer's computer system to access information contained in areas beyond the employee's access level. *Id.* at 860.

  The facts in Nosal are similar to many trade secret misappropriation cases involving current or former employees. Nosal worked for the international executive search firm Korn/Ferry but decided to leave and start his own competing business. *Id.* at 856. In the process of leaving, Nosal conspired with several fellow employees to download the names and contact information of potential clients and prospects from Korn/Ferry's confidential database. *Id.* Nosal and his fellow employees were authorized to access that database, but such access was required to be used only for company business. *Id.* Such access was not intended to be for other purposes, including to use as source material to start a competing business. *Id.*

  The government charged Nosal with 20 counts, including a violation of the CFAA for "exceed[ing] authorized access" of Korn/Ferry's database with the intent to defraud. *Id.*

The district court dismissed the CFAA count finding that the CFAA was not broad enough to reach such claims over an employee who had been authorized to access that information. *Id.* A three-judge panel of the Ninth Circuit reversed the district court's finding, but that ruling was short-lived as the Ninth Circuit granted en banc review. *Id.*

The Ninth Circuit concluded that the "CFAA does not extend to violations of use restrictions." *Id.* at 863. The Court noted that the "general purpose [of the CFAA] is to punish hacking – the circumvention of technological access barriers – not misappropriation of trade secrets." *Id.* The Court also expressed significant concerns regarding the broad reading of the CFAA advocated by the government, noting that it would create federal criminal liability based not on federal statute, but rather on employer computer use restrictions or even on a website's Terms of Use statement.

For example, the Court was concerned that a violation of the Terms of Use of the online dating service eHarmony, which prohibits the providing of "inaccurate, misleading or false information to eHarmony or any other user," could result in criminal liability for someone who "describ[ed himself] as 'tall, dark and handsome,' when [he was] actually short and homely." *Id.* at 861-62. Even though the government confirmed it would not actually prosecute a person for these purported "crimes," the panel raised concerns that a violation of the CFAA would simply be in the hands of a federal prosecutor. *Id.*

- *WEC Carolina v. Miller*, --- F.3d ---, 2012 WL 3039213 (4th Cir. July 26, 2012). The Fourth Circuit in *WEC Carolina* followed the Ninth Circuit's reasoning in *Nosal*, finding that the CFAA was not intended to criminalize violations of computer *use* restrictions. Similar to the facts of *Nosal*, the defendants in *WEC Carolina* downloaded their employer's confidential information and trade secrets several days before leaving to join a competitor. *Id.* at *1. Soon after, they used that information to make a pitch to a new client, who hired them. *Id.* at *2. WEC brought suit alleging various state law claims, as well as a CFAA count.

  The court examined *Citrin* and both the panel and *en banc* decisions from *Nosal*. The panel "reject[ed] any interpretation that grounds CFAA liability on a cessation-of-agency theory" like that adopted in *Citrin*. *Id.* at *6. Turning to *Nosal*, the court agreed that the CFAA was intended to target hackers, not disloyal employees. *Id.* at *5-6. Applying the rule of lenity because the CFAA is both a civil and criminal statute, the court adopted an interpretation of "without authorization" and "exceeds authorized access" even narrower than the Ninth Circuit, holding that they apply "only when an individual accesses a computer without permission or obtains or alters information [] beyond that which he is authorized to access." *Id.* at *6.

C. Applying the CFAA to Disloyal Employees

Both the 1st and 5th Circuits have expressly upheld violations of the CFAA by disloyal employees by virtue of "exceed[ing] authorized access," although neither court addressed the statutory ambiguity between "without authorization" and "exceeds authorized access."

- *United States v. John*, 597 F.3d 263 (5th Cir. 2010). In *John*, a bank employee conspired to charge unauthorized amounts to various customer accounts. *Id.* at 269. The defendant had access to information regarding customer accounts by virtue of her position as a bank employee, and used this information to make fraudulent charges. *Id.* The court found that the employee "was not permitted to use the information to which she had access to perpetrate a fraud," and thus the employee had violated the CFAA. *Id.* at 271. Specifically, the court concluded that an employer could place restrictions "on *the use* of information obtained by permitted access to a computer system" sufficient to establish liability under the CFAA. *Id.* (emphasis in original).

- *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001). In *EF Cultural*, a group of employees left EF Cultural to join a competitor, Explorica (the companies sold student travel tours). *Id.* at 579. At Explorica, the employees decided to compete with EF by undercutting EF's prices on each of its tours. *Id.* The former employees designed a computer program to "mine" EF's website to retrieve EF's pricing for each of their tours. *Id.* In designing this computer program, the employees utilized their knowledge of EF's website organization, tour codes, and other proprietary information. *Id.* at 582-83.

  The court found that because the former employees signed confidentiality agreements prohibiting the use or disclosure of any confidential or proprietary information, their design and use of a computer program to retrieve EF's pricing information from EF's website could be a violation of the CFAA. *Id.* at 583. Although EF's website and all information on the website was public, the former employees "exceeded [their] authorization by providing proprietary information and know-how to [create the "website mining" computer program]." *Id.*

D. Summary – A Circuit Split

The *Nosal* and *WEC Carolina* decisions demonstrate a circuit split regarding whether an employee violating her employer's computer use restrictions is subject to the CFAA. The Fifth, Seventh, and Eleventh Circuits have "interpret[ed] the CFAA broadly to cover violations of corporate computer use restrictions or violations of a duty of loyalty." *United States v. Nosal*, 676 F.3d at 862. Yet the Fourth Circuit (*WEC Carolina*) and the Ninth Circuit (*Nosal*) reject that view. Thus, depending on the jurisdiction, the CFAA may no longer be an effective tool to prevent the misuse of a company's electronic trade secrets.

Additionally, *Nosal* and *WEC Carolina* make clear that computer use restrictions are necessary but may not be sufficient to protect confidential, electronic information under the CFAA. In addition to use restrictions, companies – at least in the Fourth and Ninth Circuits – might choose to limit access to sensitive information on a need-to-know basis instead of merely limiting the appropriate use of that information. Limiting access to confidential information might not only decrease the possibility of misappropriation, but may in certain cases also preserve use of the CFAA as a litigation tool even under the narrow view of the

"without authorization" prong in the case of an employee who misuses electronic information.

II. Statute of Limitations

Civil actions under the CFAA are subject to a two-year limitations period. 18 U.S.C. § 1030(g). Courts have recognized, however, that the statute's text is not clear as to whether the limitations period accrues immediately upon a plaintiff's discovery of the damage underlying its claim or upon discovery of *both* the underlying injury *and* the identify of its perpetrator. *See Ashcroft v. Randel*, 391 F. Supp. 2d 1214, 1220 (N.D. Ga. 2005). At least one court has held that the CFAA limitations period accrues *before* a claimant has discovered all facts necessary to file its claim. *See Egilman v. Keller & Heckman, LLP*, 401 F. Supp. 2d 105, 111-112 (D.D.C. 2005). Thus, potential claimants are advised to file a claim well within two years of discovering the damage or loss caused by a potential CFAA violation.

DISCLOSURE RESTRICTIONS IN TRADE SECRET LITIGATION

I. Professional Conduct: Client Communications & Confidentiality of Information

The ABA Model Rules of Professional Conduct include rules about client communication and confidentiality that are especially important in trade secret and IP theft cases.

Rule 1.4 ("Communication") provides that:

(a) A lawyer shall:

(1) promptly inform the client of any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(e), is required by these Rules;

(2) reasonably consult with the client about the means by which the client's objectives are to be accomplished;

(3) keep the client reasonably informed about the status of the matter;

(4) promptly comply with reasonable requests for information; and

(5) consult with the client about any relevant limitation on the lawyer's conduct when the lawyer knows that the client expects assistance not permitted by the Rules of Professional Conduct or other law.

(b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

The above rule generally requires that a lawyer keep the client reasonably informed.

Rule 1.6 (“Confidentiality of Information”) separately provides as follows:

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

(b) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:

(1) to prevent reasonably certain death or substantial bodily harm;

(2) to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer's services;

(3) to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client’s commission of a crime or fraud in furtherance of which the client has used the lawyer’s services;

(4) to secure legal advice about the lawyer’s compliance with these Rules;

(5) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client; or

(6) to comply with other law or a court order.

II. Tension Between Maintaining Confidences & Keeping the Client Informed

Rule 1.4 requires that a lawyer maintain client confidences, which is heightened in trade secret cases because the client’s most valuable information may be squarely at issue. In other words, the trade secret owner seeks to recover for misappropriation of secret material while simultaneously needing the lawyer to protect this same information from further dissemination.

Yet the accused party must understand the nature of the proprietary material sufficient to prepare a reasonable defense. Further, the accused party is loath to disclose its own sensitive information. This situation gives rise to the need for protective orders with a

"counsel eyes only" designation, and this heightened confidentiality designation requires counsel to act as the client's "seeing eye dog" with respect to the most critical evidence.

In other words, in a trade secret dispute between competitors, that means that the outside lawyers – but not the clients and not even in-house counsel – see each side's trade secrets. Yet Model Rule of Professional Conduct 1.4 generally requires a lawyer to "keep the client reasonably informed about the status of the matter" and to "explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation."

In short, and depending upon the trade secrets at issue in the case, the client may in fact be barred from seeing some of the most critical evidence in the case, which in a sense is contrary to Model Rule 1.4. This tension between maintaining confidentiality and keeping the client informed presents an ethical dynamic that may be unique to trade secret and IP theft cases.

A. Limiting Access to "Highly Confidential" Information During Discovery

In cases involving highly proprietary and confidential information, courts often find that even in-house counsel should be restricted from reviewing the most sensitive material produced by the opponent, at least in instances in which the in-house lawyer is found to be involved in the organization's competitive "decision-making" and in which the risks of inadvertent disclosure (to others in the organization) is high. *See Autotech Techs. Limited P'ship v. Automationdirect.com, Inc.*, 237 F.R.D. 405 (N.D. Ill. 2006).

Autotech involved the claims of a distributor of touch-screen computer panels against the manufacturer of the computer panels. The manufacturer argued that its in-house counsel should be allowed to review the distributor's confidential customer information without redactions in order to assist fully with the litigation. *Id.* at 406. The distributor-plaintiff resisted unfettered access by the manufacturer's in-house counsel to the distributor's confidential customer information and insisted upon production of the information in redacted format. *Id.*

While recognizing that "in-house counsel are members of the bar" and that they "are bound by the same canons of ethics as other lawyers," the court explained that "house counsel are subject to pressures different from those which outside counsel face," because "their own economic well-being is inextricably bound up with their employer's." *Id.* at 407. According to the court, "[t]he sole question is whether there is an unacceptable risk of or opportunity for 'inadvertent disclosure' of confidential information." *Id.* An "analysis of the risk of 'inadvertent disclosure' involves an assessment of the entire setting in which in-house counsel functions," *id.* at 407-08, including "a careful and comprehensive inquiry into in-house counsel's actual (not nominal) role in the affairs of the company, his association and relationship with those in the corporate hierarchy who are competitive decision makers, and any other factor that enhances the risk of inadvertent disclosure." *Id.* at 408. *See also Intel Corp. v. VIA Techs., Inc.*, 198 F.R.D. 525, 530 (N.D. Cal. 2000) (limiting access where in-

house counsel reported directly to vice president involved in competitive decision-making and when vice president's access had been restricted).

In addressing this issue, courts do not struggle with the good faith of in-house counsel, or in-house counsel's ability to comply with the ethical rules, but instead with the risk of "inadvertent disclosure" inside the organization. *See, e.g., Andrx Pharms., LLC v. GlaxoSmithKline, PLC*, 236 F.R.D. 583, 585-86 (S.D. Fla. 2006) ("Even if the competitor's counsel acted in the best of faith and in accordance with the highest ethical standards, the question remains whether access to the moving party's confidential information would create 'an unacceptable opportunity for inadvertent disclosure'"); *Nazomi Communications, Inc. v. ARM Holdings PLC*, No. C02-2521-JF, 2002 WL 32831822, *3 (N.D. Cal. Oct. 11, 2002) (leading cases in this area presuppose fidelity to ethical duties and bar access only when there is a significant risk of inadvertent disclosure).

"Attorneys' eyes only" information generally may be shared only with *independent* outside counsel. In other words, if outside counsel serves dual roles, such as corporate secretary and / or board member for a corporation, the outside attorney may be denied access to counsel eyes only materials. For example, *Norbrook Laboratories Ltd. v. Hanford Manufacturing Co.*, No. 5:03-CV-165, 2003 U.S. Dist. LEXIS 6851 (N.D. N.Y. 2003), a trade secret dispute between two drug manufacturers, involved an outside counsel who served as both corporate secretary and a member of the board of directors. *Id.* at *13. The court concluded that the outside lawyer's multiple roles "present an unacceptable opportunity for the inadvertent disclosure of confidential information." *Id.* at *16. Even though the outside lawyer pledged to maintain the confidentiality of the information at issue, the court reasoned that "it cannot endorse a situation that places [the lawyer's] ethical obligations as an attorney in direct competition with his fiduciary duty" to his employer. *Id.* The court also observed that "it is very difficult for the human mind to compartmentalize and selectively suppress information once learned, no matter how well intentioned the effort may be to do so." *Id.*

Parties should use not over-use the "attorney's eyes only" designation and it should be utilized with limitation and in good faith. Courts are often inclined to order de-designation of materials that do not warrant an "attorney's eyes only" designation. For example, in *Team Play, Inc. v. Boyer Sky Boy Productions, Inc.*, No. 03-C-7240, 2005 U.S. Dist. LEXIS 3968 (N.D. Ill. Jan. 31, 2005), a party marked roughly 4,000 out of 6,000 documents as "highly confidential" and thereby restricted opposing counsel from sharing the documents with the client. The documents marked "attorneys' eyes only" consisted mainly of sales invoices and accounting information related to the plaintiff's damage claim, and had the consequence of preventing defense counsel "from discussing the damages aspect of his case" with the client and leaving the client with no information from which "to make an intelligent decision as to what a reasonable settlement figure might be." *Id.* at *4.

"Where a party's use of the Attorneys' Eyes Only designation is sweeping it can be a form of discovery abuse and result in the blanket modification of a protective order as well as the imposition of sanctions on the designating party." *Id.* at *3. In *Team Play*, the court

ordered removal of the "attorney's eyes only" designation for *all* documents produced by the plaintiff but on the condition that the defendant's client submit a detailed statement affirming representations by his counsel about his non-involvement in the industry and his lack of intention to re-enter the market. *Id.* at *6-7.

B. "Highly Confidential" Information at Trial

While protective orders may successfully limit distribution of trade secrets and proprietary information during discovery, protective orders are less reliable for trials and evidentiary proceedings. For example, some courts are skeptical of the capacity of *any* protective order to preserve the confidentiality of materials used at trial. For example, the court in *Mannington Mills, Inc. v. Armstrong World Industries, Inc.*, 206 F.R.D. 525, 529 (D. Del. 2002), held, in connection with a subpoena to a non-party, that "discovery is not allowed where no need is shown, or where compliance is unduly burdensome, or where the potential harm caused by production outweighs the benefit." The party seeking the discovery in *Mannington* argued that no showing of harm could be made based on a court-ordered protective order that limited disclosure of confidential information to attorney's eyes only. *Id.* at 530. Rejecting that argument, the court observed that what happens with any confidential information at trial "*is anyone's guess*." *Id* (emphasis added). The court further stated that "it would be divorced from reality to believe that either party here would serve as the champion of its competitor . . . to maintain the confidentiality designation or to limit public disclosure . . . *during trial*." *Id* (citations omitted and emphasis added). *See also Team Play, Inc. v. Boyer Sky Boy Productions, Inc.*, No. 03-C-7240, 2005 U.S. Dist. LEXIS 3968, *6 (N.D. Ill. Jan. 31, 2005) (ordering de-designation of documents improperly marked attorney's eyes only" and noting "that once this case goes to trial, the documents will become part of the public record in any event").

APPENDIX

CHECKLIST FOR GUARDING AGAINST LOSS OF TRADE SECRETS

☑ ***Identify most valuable confidential information:*** Assess information deemed to be the most confidential, such as customer purchasing histories, formulas, secret recipes, etc., for purposes of making certain that the most valuable information is adequately protected.

☑ ***Confidentiality and non-disclosure commitments:*** Require employees to execute confidentiality agreements and non-disclosure obligations that apply during employment and that survive post-separation; send post-employment letters to former employees and new employers about non-disclosure obligations.

☑ ***Policy and procedure training:*** Conduct initial and recurring training sessions about company policies regarding confidentiality; educate employees about the existence of trade secrets.

☑ ***No personal gain:*** Adopt company policy making clear that employees are not authorized to use company information and data at any time for personal gain. Communicate the policy!

☑ ***Post-employment covenants:*** Use restrictive covenants (noncompetition agreements) with key employees who have access to the most sensitive information.

☑ ***Limit employee access:*** Restrict physical access to the most sensitive materials. Implement additional password-protected access (VPN, encryption, firewalls, etc.) to the most sensitive electronic data.

☑ ***Need to know basis:*** Prohibit distribution of critical information except to employees with a clear need for the information.

☑ ***"Confidential" designations:*** Use "confidential" legends and warnings on documents.

☑ ***Facility and premises access:*** Regulate visitor access to facilities.

☑ ***Trace document copies:*** Use copy protection policies and embedded codes to trace copies.

☑ ***No downloading company information:*** Limit or restrict the use of external hard drives or other outside media for downloading company information.

☑ ***Employees to comply with prior obligations:*** Tell new employees that they are expected to comply with ongoing confidentiality obligations in favor of prior employers and scope of employment does not include use of unauthorized trade secrets.

☑ ***Exit interviews:*** Conduct rigorous exit interviews when employees separate in order to confirm that employees have returned all company property and have not retained any confidential company information in any format.

☑ ***Disable access promptly:*** Promptly disconnect network access of departing employees; if suspected, immediately check for signs of misappropriation.

SAMPLE EXIT INTERVIEW FORM
(TO BE COMPLETED PRIOR TO DEPARTURE)

INTRODUCTION

We understand that you will be ending your employment with the Company on _____[date]. You remain a Company employee until that date and should not begin performing any work for your new employer until after that date, whether during or after business hours. As you prepare to leave, we ask that you complete this Exit Interview/Checkout Form. It will assist us in processing your exit and accounting for various types of Company property you may have received prior to your departure.

EQUIPMENT AND ACCESS TOOLS

We need to ensure that all of our equipment has been returned to the Company, please respond to the following:

		Returned?		Never Issued
1.	ID Card	Yes ☐	No ☐	☐
2.	Corporate Credit Card	Yes ☐	No ☐	☐
3.	Facility Access Card/keys	Yes ☐	No ☐	☐
3.	Corporate Calling Card	Yes ☐	No ☐	☐
4.	Company Cell Phone	Yes ☐	No ☐	☐
5.	Company Laptop or Other Computer Equipment	Yes ☐	No ☐	☐
6.	Company Thumb Drive/Zip Drive/External Hard Drive	Yes ☐	No ☐	☐
7.	Company PDA/Blackberry	Yes ☐	No ☐	☐
8.	Other _____	Yes ☐	No ☐	☐

Initials _____

DOCUMENTS/FILES/RECORDS

As an employee of X Company you had access to various documents, reports, and information that the Company considers proprietary and confidential – in both electronic and paper form. The Company needs to confirm that all of its property has been returned or deleted from non-Company storage media (CDs/DVDs, portable hard drives, thumb drives, personal handheld devices, cell phones, smart phones, personal e-mail accounts, personal desktop computers, personal laptop computers, and the like) and that none of these items have been disclosed to persons outside of the Company. We have listed below some of the most confidential documents of the Company; by listing some documents here but not others

we do not mean to suggest that other Company documents are not confidential. Please respond to the following:

Examples of Documents—Have You Received or Been Given Access to the Following Materials?

1.	[Annual Strategic or Sales Plan]	Yes ☐ No ☐
2.	[Customer List]	Yes ☐ No ☐
3.	[Customer Profiles]	Yes ☐ No ☐
4.	[Research Notebooks or Plans]	Yes ☐ No ☐
5.	[Other relevant core Company documents]	Yes ☐ No ☐

*Did you copy or e-mail any of these documents? Yes ☐ No ☐

*Did you disclose or transfer any of this information to anyone outside of the Company? Yes ☐ No ☐

*Are you currently in possession of any of these documents? Yes ☐ No ☐

*If the answer to any of these questions is yes, please explain:

_____

_____

_____

If during the course of your employment, you transferred any Company documents (not limited to the documents listed above) to non-Company storage media (such as CDs/DVDs, portable hard drives, thumb drives, and the like), personal handheld devices, cell phones, smart phones, personal e-mail accounts, or personal desktop or laptop computers, please identify all such media, devices, e-mail accounts, or computers and their location. We will discuss with you how to ensure that all such materials are returned or properly deleted from non-Company media.

_____

_____

_____

Have you returned all X Company confidential and proprietary documents? Yes ☐ No ☐

If so, to whom, when, and how? _____ Yes ☐ No ☐

_____

_____

Initials _____

CODE OF CONDUCT

As you know, the Company takes its Code of Conduct very seriously. The Code of Conduct provides, among other things, that employees shall not use corporate property or information for personal gain. You have acknowledged your compliance with this Code. A copy is attached.

Initials _____

EMPLOYEE INVENTION AND TRADE SECRET AGREEMENT

As you know, your relationship with the Company is governed by an Employee Invention and Trade Secret Agreement you entered into with the Company (copy attached). This Agreement provides that, in your employment after leaving, you will not disclose, without the Company's written consent, any secret or confidential information obtained during your employment with the Company.

Based on your commitments to the Company, there may be situations in the course of your new employment in which you simply cannot participate in a project without necessarily using the confidential information you have learned about the Company. In those situations, your agreement with the Company requires that you excuse yourself from those specific projects. In other circumstances, it may be most effective for you to simply assign responsibility for particular projects to other individuals, acting without your guidance. There may be situations in which you are not certain whether information you know and would like to use in your work with your new employer is in fact confidential information of the Company. In those circumstances, we ask that you contact at the Company to discuss the issue and arrive at an appropriate resolution that will respect your continuing obligations to the Company.

Your obligation not to disclose, without the Company's prior written consent, any secret information obtained during the course of your employment with the Company, remains in effect for as long as such information remains a trade secret under applicable law.

Your obligation not to disclose, without the Company's prior written consent, any confidential or proprietary information obtained during the course of your employment with the Company, remains in effect for [INSERT SET TERM FROM AGREEMENT] years.

Initials _____

OTHER AGREEMENTS

Your post-employment obligations are also governed by the [INSERT NAME OF AGREEMENT]. A copy of this Agreement is attached. If you have any questions about this Agreement, please contact _____.

Initials _____

NEW EMPLOYMENT

Have you accepted other employment?

If so, with what company? _____

What will be your new title? _____

When is your anticipated start date? _____

What is your contact information? (phone, email and physical address)?

Phone: _____
Email: _____
Address: _____

Initials _____

Please take a moment to ensure that your answers above are accurate. Again, we thank you for completing this form and assisting with our on-going efforts to protect our confidential and proprietary information. We thank you for your services.

Dated: _____

_____
[Executive Signature]

_____
[Print Name]

SAMPLE ACKNOWLEDGEMENT REGARDING TRADE SECRETS AND PROPRIETARY INFORMATION FOR INCOMING EMPLOYEES

I understand and acknowledge that it is the policy of X Co. and its affiliates (the "Company") to respect the trade secrets, inventions and other proprietary and confidential information ("Confidential Information") belonging to third parties. Therefore, in addition to agreeing not to disclose or use Confidential Information belonging to the Company in violation of any applicable confidentiality agreement or Company policies as may be in effect or amended from time to time, as a condition of employment with the Company, I hereby represent and agree as follows:

1. I am not subject to any agreement of any kind with any prior employer or other person or entity relating in any way to my right or my ability to be employed by and/or to perform services for the Company.

2. The Company has instructed me not to bring to, disclose to or use in connection with my employment or potential employment with the Company any Confidential Information from any prior employer or other person or entity.

3. I have not brought to, disclosed to or used in connection with my employment or potential employment with the Company any Confidential Information from any prior employer or other person or entity.

4. I will not bring to, disclose to or use in connection with my employment with the Company any Confidential Information from any prior employer or other person or entity.

5. During my employment with the Company and thereafter, I will not take, disclose or use any Confidential Information acquired as a result of my employment with the Company, except as authorized by the Company.

_____
Employee's Printed Name

_____
Employee's Signature

_____
Date

SAMPLE POLICY LANGUAGE CONCERNING USE OF COMPANY PROPERTY AND "NO PERSONAL GAIN"

The Company provides us with a wide variety of resources, such as computers, communication devices and other equipment and materials, for use in conducting company business. The Company allows our personal use of these resources from time to time provided that this usage is kept to a minimum and is in compliance with company policy. Excessive personal use of company resources increases company costs and expenses, reduces the availability of the resources for business use and may adversely affect our job performance.

- We do not use any Company resource in violation of any law, company policy or these Standards.
- We safeguard the Company's resources in order to protect these items from theft or misuse.
- We do not use any Company resource excessively for personal use.
- We do not use any Company resource for personal activities which may lead to the loss of damage of the asset.
- We do not use any Company resource to create, transmit, store or display solicitations, chain letters, or messages, images or materials that are for personal gain or are threatening, sexually explicit, harassing, or otherwise demeaning to any person or group.
- We have no expectation of personal privacy in any Company resource used by us for personal activities including Company computers, servers and systems, telephones, voicemail systems, offices, desks, cabinets, vehicles or other equipment belonging to the Company. This applies to any messages or records created, stored or transmitted by us using Company systems, including electronic documents such as e-mail and voicemail.

SAMPLE SOFTWARE PURCHASING GUIDELINES & CHECKLIST

This type of information should be collected for all software purchases and it is recommended to continue this type of documentation when the licenses are increased, decreased, migrated, or maintenance is renewed. This form should be helpful during version upgrades, version retirement, realignment of software suites, etc.

A. If a master software license agreement has not been completed, one should be negotiated and executed.

B. Two (2) other documents should be generated for each software program purchased, (1) the license grant document and (2) the "Schedule." Both documents could be combined into one document, the "Schedule." The two (2) documents, or the combined document, are normally signed by the purchaser and the vendor.

Information Contained in the Schedule:

- Name of software product and/or suite.
- Description of each software product (including names within a suite) purchased including version number.
- Location of use (ex, ----, state, country, or Enterprise-wide or Globally).
- Contact information for company's purchaser and for vendor's contact.
- Pricing:
  - List price of each software product purchased
  - Discounted price for the software version and number of licenses
  - Difference between 1 and 2 above
- License grant (or EULA) if not listed in a separate document.
- Procedure and restrictions for entitlement of software/product version upgrade.
- Process for recouping licenses that may be attached to individuals or equipment.
- Scheduled delivery date.
- Method of delivery (CD or download or other).
- Backup copies allowed for disaster recovery.
- Whether software may be used by contractors or outsourced service organizations.
- Warranty period: start and end dates.
- Maintenance
  - Maintenance fee must be listed. (Fee should be negotiated to be a percentage of the discounted price, not the list price).
  - Start and end date of the maintenance period (Ideally, the maintenance fee period should start after the warranty period is completed).
  - If software implementation is to be implemented in phases for multiple sites, language should clarify if a single start and end date for maintenance for all phases had been negotiated.

Indicate with a yes all that apply (in the table below) for each software product purchased.

A	B	C
If Column B is relevant for the software purchased indicate by entering Yes below	**License grant (usage) allowed**	**Additional Information required, if relevant**
	Named user	If yes, can license be transferred if user obtains another job, leaves company, etc.
	Concurrent	List number of concurrent users allowed if designated in the license grant
	Instance Based	Type of capacity or number of servers
	Change Users	Allows changes to users (increase and/or decrease total numbers)
	User	Special definitions of users (person, machine, IP address)
	By designated machine (s)	List machine model (s)
	By designated location(s) only	List location(s)
	Regional use	
	Enterprise wide	
	Affiliates / Subsidiaries	
	Server	List number allowed
	Virtual Server	List number allowed
	Virtualized Desktop Interface	List concurrent or instance based

A	B	C
If Column B is relevant for the software purchased indicate by entering Yes below	**License grant (usage) allowed**	**Additional Information required, if relevant**
	Buffer	A +/- number of licenses allowed and for what amount of time.
	Cluster	Groups of Servers
	Server Types	Different prices or restrictions for production, backup, and disaster recovery servers.
	Managed Software	Software includes administrative controls that prevent license misuse.
	Languages	
	Website and/or wireless use	Indicate what is allowed regarding use, transformation, distribution, and downloading
	Perpetual, subscription, or time limited	If time limited, for what period (i.e. temporary).

