THE SEDONA CONFERENCE WORKING GROUP SERIES

wgs

THE SEDONA CONFERENCE

Commentary on Protecting Trade Secrets Throughout The Employment Life Cycle

A Project of The Sedona Conference
Working Group on Trade Secrets (WG12)

JUNE 2021
PUBLIC COMMENT VERSION
Submit Comments by September 30, 2021,
to comments@sedonaconference.org

The Sedona Conference

The Sedona Conference Commentary on Protecting Trade Secrets Throughout The Employment Life Cycle

A Project of The Sedona Conference Working Group (WG12) on Trade Secrets

JUNE 2021 VERSION

Author:	The Sedona Conference	
Editors-in-Chief:	James Pooley Victoria Cundiff	
Managing Editor:	Jim W. Ko	
Senior Editors:	Russell Beck John Marsh Robert Milligan	
Contributing Editors:	Barry Brown Rebecca Edelson Stacey Schmidt Karen Tompkins James Vaughn	Richard Dole Julie McCarthy Steve Stawski Danielle Vanderzanden Robert Yonowitz
Judicial Advisors:	Hon. Gail Andler (ret.) Hon. Hildy Bowbeer	

We thank all of our Working Group Series Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, click on the "Sponsors" navigation bar on the homepage of our website.

REPRINT REQUESTS:
Requests for reprints or reprint information should be directed to Craig W. Weinlein, Executive Director, The Sedona Conference, at info@sedonaconference.org or 602-258-4910.

Preface

Welcome to the June 2021 Public Comment Version of The Sedona Conference *Commentary on Protecting Trade Secrets Throughout The Employment Life Cycle*, a project of The Sedona Conference Working Group on Trade Secret Law (WG12). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, intellectual property rights, and data privacy and security law. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The mission of WG12, formed in February 2018, is "to develop consensus and nonpartisan principles for managing trade secret litigation and well-vetted guidelines for consideration in protecting trade secrets, recognizing that every organization has and uses trade secrets, that trade secret disputes frequently intersect with other important public policies such as employee mobility and international trade, and that trade secret disputes are litigated in both state and federal courts." The Working Group consists of members representing all stakeholders in trade secret law and litigation.

The WG12 *Commentary* drafting team was launched in November 2018. Earlier drafts of this publication were a focus of dialogue at the WG12 Annual Meeting, Online, in November 2020, the WG12 Annual Meeting in Charlotte, North Carolina, in November 2019, the WG12 Inaugural Meeting in Los Angeles, California, in November 2018, and the Inaugural Sedona Conference on Developing Best Practices for Trade Secret Issues in Scottsdale, Arizona, in December 2017. The editors have reviewed the comments received through the Working Group Series review and comment process.

This *Commentary* represents the collective efforts of many individual contributors. On behalf of The Sedona Conference, I thank in particular James Pooley, the Chair of WG12, and Victoria Cundiff, the Vice-Chair of WG12, who serve as the Editors-in-Chief of this publication, and Russell Beck, John Marsh, and Robert Milligan, who serve as the Senior Editors of this publication. I also thank everyone else involved for their time and attention during this extensive drafting and editing process, including our Contributing Editors: Barry Brown, Richard Dole, Rebecca Edelson, Julie McCarthy, Stacey Schmidt, Steve Stawski, Karen Tompkins, Danielle Vanderzanden, James Vaughn, and Robert Yonowitz.

The drafting process for this *Commentary* has also been supported by the Working Group 12 Steering Committee and Judicial Advisors. The statements in this *Commentary* are solely those of the nonjudicial members of the Working Group; they do not represent any judicial endorsement of any recommended practices.

Please note that this version of the *Commentary* is open for public comment through September 30, 2021, and suggestions for improvements are welcome. After the deadline for public comment has passed, the drafting team will review the public comments and determine what edits are appropriate for the final version. Please send comments to comments@sedonaconference.org or fax them to 602-258-2499.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG12 and several other Working Groups in the areas of electronic document management and discovery, cross-border discovery and data protection laws, international data transfers, data security and privacy liability, patent remedies and damages, and patent litigation best practices. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be.

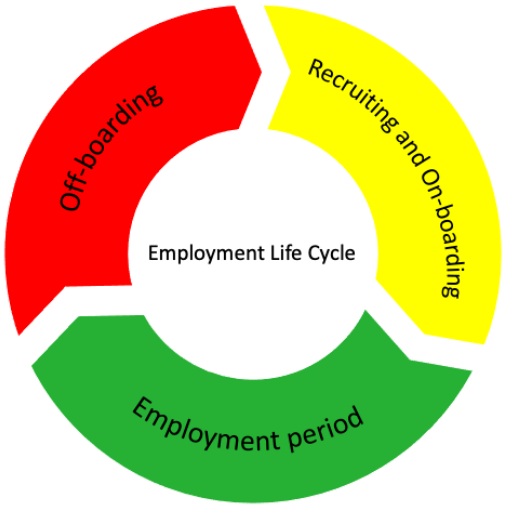
Craig W. Weinlein
Executive Director
The Sedona Conference
June 2021

Foreword

Employees are at the center of most aspects of trade secrets: Trade secrets cannot exist without the work of employees, cannot be protected without the efforts of employees, and would rarely be compromised or lost without the conduct of employees. This *Commentary* focuses on the inherent potential tensions this creates in the employer-employee relationship.

While in most circumstances, employers and employees will be aligned in protecting trade secrets for their mutual benefit at the beginning and during the employment relationship, there remains an inherent tension between an employer's interest in protecting its trade secrets and an employee's interest in engaging in future employment. This tension is further complicated by the fact that, although the departing employee is at the end of one employment life cycle, they are typically simultaneously at the beginning of the next, where the former's employer's risk of compromise or loss of its trade secrets corresponds directly to the new employer's risk of infiltration of those same trade secrets.

This *Commentary* addresses these issues through a chronological view of the employment relationship, from recruiting and on-boarding, to the period of employment, to the off-boarding, and back to the on-boarding, as follows:



The editors would like to express their appreciation to the members of the drafting team and the judicial advisors for their valuable input and thoughtful commentary.

James Pooley
Victoria Cundiff
Editors-in-Chief and Working Group 12 Steering Committee Chair and Vice-Chair

Russell Beck
John F. Marsh
Robert B. Milligan
Senior Editors

Table of Contents

The Employment Life Cycle Relating to Trade Secrets Principles "At a Glance"

The Employment Life Cycle Relating to Trade Secrets Guidelines "At a Glance"

I. Introduction

The natural dynamics of trade secret law reveal inherent potential tensions in the employer-employee relationship. Employers typically share trade secrets with their employees. In most circumstances, employers and employees will be aligned in protecting that information for their mutual benefit, with employers enabling employees to use the information to do their job as effectively as possible for the benefit of the organization, and with employees using the information to maximize their advancement within the organization.[1]

However, a significant portion of trade secret lawsuits arise in the context of the former employer-former employee relationship.[2] Survey data and studies reinforce the role that employees may play in loss of employers' control over confidential information. A frequently cited study by Symantec Corporation found that half of employees who left their jobs kept confidential data of their former employers.[3] That study also showed that most employees who were surveyed did not believe this conduct was wrong and thought their actions were appropriate because they caused no harm to their former employers. Roughly the same number claimed that the company failed to enforce policies applicable to data protection.

The tensions between employers and employees are rooted in the very nature of trade secrets. As one court has observed, "[a] trade secret is one of the most elusive and difficult concepts in the law to define. In many cases, the existence of a trade secret is not obvious; it requires an ad hoc evaluation of all the surrounding circumstances."[4] This elusive quality results from at least these characteristics: (1) broad categories of information may be included and protected as trade secrets; (2) what qualifies as a trade secret can potentially change and evolve over time; (3) the value of information may range from "crown jewels" to ephemeral data of minimal value but that technically qualifies as a trade secret; and (4) unlike other forms of intellectual property, there is no definitive registry of information that determines the parameters and ownership of a trade secret.

Given the imprecise contours of trade secrets, many employers are unaware of their exact metes and bounds relative to the "general skill, knowledge, and experience" applied by their employees. But it should generally be assumed that employers have some protectable trade secrets even if their precise scope is not defined. Indeed, employers not only have the right to establish policies designed to protect their potential trade secrets, but must do so to preserve their ability to enforce them in the courts. It is incumbent on employers to reasonably define for their employees the types of

---

1 This *Commentary* is intended to address only the sharing and protection of trade secrets during the employment life cycle and does not address the sharing or protection of other information that may be deemed confidential by statute or contract (i.e., personal identifiable information, information protected by HIPPA or some other state or federal statute, or other information protected by a contract that may not otherwise qualify as a trade secret).

2 In over 85 percent of the trade secret cases filed in federal court from 1950 to 2008 that had a written opinion based on trade secret law, "[t]he alleged misappropriator was someone the trade secret owner knew—either an employee or business partner." David Almeling, et al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZAGA L. REV. 291, 294 (2010).

3 Symantec Corp., *Data Loss During Downsizing*, https://investor.nortonlifelock.com/About/Investors/press-releases/press-release-details/2009/More-Than-Half-Of-Ex-Employees-Admit-To-Stealing-Company-Data-According-To-New-Study/default.aspx [hereinafter *Symantec IP/Employees Study*].

4 Learning Curve Toys, Inc. v. PlayWood Toys, Inc., 342 F.3d 714, 723 (7th Cir. 2003).

information they treat as their trade secrets, and it is generally incumbent on employees to help protect such information from improper use or disclosure. But challenging questions can arise, particularly when employees departs for a competitor.

The following introduction identifies and frames these issues, explains the forces that shape the potential conflicts, and provides consensus principles and guidelines to mitigate against disputes.

A. THE EMPLOYER'S PERSPECTIVE

There is a central paradox surrounding the role of trade secrets in the employment life cycle. On the one hand, employers need to disclose trade secrets to their employees in order to operate. On the other hand, employees often pose the greatest risk to those trade secrets.

More specifically, it is in the interest of employers to ensure that their employees are productive and successful throughout their employment. Therefore, during the course of the employment life cycle, employers will provide their employees with access to secret information to enable them to effectively perform their jobs. For example, a manager will typically be given internal financial information, budgets, forecasts, and strategic plans to implement. An engineer may be provided with historical information about the successes and failures in the design and development of the employer's products. And their employers will often expect these employees to use and build upon those trade secrets for the benefit of the organization.

Relatedly, employees may be hired for the purpose of improving or creating information that qualifies as a trade secret. For example, employees involved in research and development are generally expected to improve or develop new products, processes, or services, while sales representatives may be expected to gather and compile information about the current or future needs of existing or new customers.

Employers should take steps to facilitate a mutual trust with their employees regarding the protection of trade secrets. Employers reasonably expect that their employees will maintain confidentiality (including of information entrusted to the company by third parties) and avoid use of sensitive information for any purpose outside the defined parameters of their employers' businesses. While employers should develop, implement, monitor, and enforce trade secret protection policies, all organizations necessarily rely on their employees to follow those policies and to exercise appropriate care and judgment in connection with their use or disclosure of trade secrets.

But disclosure to employees of an organization's trade secret information necessarily puts it at risk. This follows from the simple reality that the vast majority of employees will ultimately leave to work elsewhere. Some will leave under less than amicable circumstances, and many will naturally transition to work for a competitor. These circumstances create a risk that former employees will not only (properly) use skills developed or honed while working for their former employers, but also (improperly) use or disclose their former employers' trade secrets. As reflected in the study referenced above, many employees may have a cavalier attitude about their employers' trade secret information, believing it acceptable to take and use it in future employment.[5] Normally this results not from malice but from misunderstanding concerning what belongs to the company and what

[5] *See Symantec IP/Employees Study*, *supra* note 3.

their obligations are. Other employees may assume, incorrectly, that if they did not take or retain any of their employers' documents, they no longer have to concern themselves with protecting trade secrets. Any company that has valuable trade secret information should take measures to mitigate against all these risks.

A related concern for hiring employers is having access to a talent pool to further their business objectives while at same time respecting the obligations of candidates to their prior employers, as well as any enforceable restrictive covenants. Hiring employers should have the ability to recruit lawfully without the fear of facing anticompetitive, bad-faith claims calculated to stifle employee mobility. However, former employers deserve protection against competitors who use hiring as a means to secure improper access to trade secrets, as well as against former employees who use trade secrets for their own or their new employer's benefit.

Given these realities, employers should—throughout the entire employment lifecycle, from hiring through offboarding—explore all reasonable avenues for protecting against these risks to their trade secret assets.

B. THE EMPLOYEE'S PERSPECTIVE

From the employee's perspective, the relationship with their employers reflects an inherent imbalance of power. This is understandable, given that it is the employers that draft employment agreements and policies, typically in a take-it-or-leave-it fashion. This creates the potential for employer overreach, using that imbalance of power to dictate unreasonable terms.

Indeed, employers often have the ability to impose terms that can substantially impact their employees' future mobility through restrictive agreements. For example, employers may present an employment agreement with restrictive covenants on the employee's first day of work, after the employee has quit a previous job and has no practical leverage to negotiate the terms. In many states, employers are even permitted to amend agreements during the course of employment to add restrictive covenants, with the only consideration being the continuation of at-will employment.

Finally, employers may (and often do) take a broad view of the information entitled to protection. But employees may bring with them deep and relevant prior knowledge, referred to as "general skill, knowledge, and experience." This baseline expertise is the employee's primary contribution to the relationship and should be the employee's to keep and use in a subsequent position. However, when those skills are brought to bear or become enhanced on the job, a dispute may arise over whether the resulting information belongs to the employer or is properly accretive to the employee's general skill, knowledge, and experience.

In this inherently ambiguous environment, it may be tempting for some employers to overreach by taking an unjustifiably broad view of what information may be entitled to trade secret protection. Examples of such overreach may include:

1.) Asserting ownership, through employment agreements or policies, of all information to which employees had access or which employees used to create something for their employers.

2.) Asserting ownership of all information that relates to the company's business, regardless of whether it is known within the industry.

3.) Defining as a trade secret everything that employees worked on during the period of employment.

Whether some of this information may be properly claimed as a trade secret by employers may depend on the governing law. However, while employees may challenge such broad claims, the relative imbalance of power and resources may make that impractical, affecting not only employees but also the legitimate interest of competitors that may otherwise have considered offering them alternative employment.

From the employees' perspective, in addition to the general skills, knowledge, and experience that they possessed prior to hire, they may also claim learned general skills and knowledge on the job to be equally transferrable to their new employers.[6] The line of demarcation between an employer's trade secret and an employee's general skill, knowledge, and experience can be murky, particularly where the employee has applied that general skill, knowledge, and experience in the creation of a valuable asset. Given the complexities of defining the boundaries and value of trade secrets, it may be difficult to discern in any specific case whether an employer's attempt to enforce its alleged rights is made in good faith or is animated by anticompetitive or other inappropriate motives.

*****

For these reasons, employer-employee disputes over trade secrets are frequently emotional and contentious. This should come as no surprise, given the potential impact such disputes may have both on information an employer may consider critical to its enterprise and on an employee's ability to find better opportunities. The emotional overlay is only intensified by the charges they typically level at each other: charges by the employer of stealing and betrayal, countered with charges by the employee of overreaching and anticompetitive behavior.

[6] *See, e.g.,* SI Handling Sys., Inc. v. Heisley, 753 F.2d 1244, 1267 (3d Cir. 1985) ("[A]n employee's general knowledge, skill, and experience are not trade secrets. Thus in theory an employer generally may not inhibit the manner in which an employee uses his or her knowledge, skill, and experience—even if these were acquired during employment." (citations omitted) (analyzing information in suit in detail and finding that some constitutes trade secrets and that other information is simply knowledge, skill and experience the employee is free to use); Pressure Sci., Inc. v. Kramer, 413 F. Supp. 618, 629 (D. Conn. 1976) (holding that an employee cannot be barred from using his general skill and experience in the industry), *aff'd*, 551 F.2d 301 (2d Cir. 1976); George O'Day Assocs., Inc. v. Talman Corp., 206 F. Supp. 297, 300 (D.R.I. 1962) ("[A]n employee after leaving the service of an employer may carry on the same business on his own and use for his own benefits the things he has learned while in the earlier employment." (quoting Midland-Ross Corp. v. Yokana, 293 F.2d 411, 412 (3d Cir. 1961))), *aff'd*, 310 F.2d 623 (1st Cir. 1962); Van Prods. Co. v. General Welding & Fabricating Co., 213 A.2d 769, 776 (Pa. 1965) (holding that an employee "is entitled to take with him 'the experience, knowledge, memory, and skills which he gained while . . . employed'") (internal citation omitted).

C. BALANCING THE INTERESTS OF EMPLOYERS AND EMPLOYEES IN PROTECTING TRADE SECRETS

As noted above, defining the legally protectable metes and bounds of a company's trade secrets is inherently challenging and ultimately may only be accomplished with certainty by the courts through the litigation process.

Some employers may tend to overreach by expansively defining what constitutes the company's trade secrets, as a result of which their enforcement efforts may inappropriately restrict their former employees' application of their general knowledge, skill, and experience, and thus their employment mobility. For example, a company in the driverless car industry cannot reasonably assert as its trade secret "how we design and manufacture our driverless cars," because the uncertainty of its sweep could effectively preclude the employee from working for any other driverless car company.

Some employees may overreach by more broadly defining what constitutes their general knowledge, skill, and experience to include nonpublic, valuable information that is properly understood by the employer as its trade secrets. For example, a code developer may have coding experience that represents general skill, knowledge, and experience, but working on the company's project and applying that knowledge to create code specific to the project could involve, or lead to the creation of additional, company trade secrets.

The following set of four Principles address both tendencies and provide guidance for employers and employees to manage these trade secret issues in a balanced fashion, accounting for the interests of all parties concerned.

The consensus of WG12 is that trade secret protection in the employment life cycle be governed by the following key principle:

> **<u>Principle No. 1</u> – There is an inherent tension between an employer's interest in protecting its trade secrets and an employee's interest in engaging in future employment. Employers should tailor their policies and procedures to guard against the risk of unlawful use or disclosure of their trade secrets, while avoiding inappropriately restricting their former employees' application of their general knowledge, skill, and experience in their next employment.**

This overarching Principle recognizes two primary competing interests in the employment life cycle—protection of an employer's trade secrets and an employee's mobility—and strives to promote balance between them. Employers may have the legal right to include broad protections available to them in their employee agreements and policies to protect against potential risks. However, if unchecked, such a practice may be not only contrary to Principle No. 1, but also counterproductive for employers by damaging their relationships with those tasked with protecting those trade secrets, or in some cases even potentially leaving the employers subject to liability.[7]

[7] Several courts have treated overly broad employee nondisclosure agreements as restrictive covenants and declined to enforce them. *See* TLS Mgmt. & Marketing Servs., LLC v. Rodriguez-Toledo, 2020 WL 4187246 (1st Cir. July 21, 2020); Robinson v. U-Haul Co. of Cal., 4 Cal. App. 5th 304 (Oct. 18, 2016).

Company counsel should consider having frank conversations with the company's leadership on the appropriate balance between maximum trade secret protections and employee mobility and related intellectual property rights. Key questions to consider may include:

- What are examples of the company's "crown jewels"—the specific trade secret information from which the company derives significant competitive advantage in the marketplace and that do not include employee general knowledge, skill, and experience—that the company should affirmatively protect with restrictions on future employment by its employees?

- Are the company's protection measures proportionate— i.e., tailored to the company's particular business, the value and vulnerability of its trade secrets, and its employees' roles and means of access? Or will some measures unduly interfere with the ability of employees to do their jobs and ensure that the business fully benefits from its trade secrets?

- Would the company benefit from a discussion with departing employees distinguishing what are the company's protectable trade secrets from the general knowledge, skill, and experience that the employees may use in future employment?

WG12 further presents the following additional Principles in furtherance of Principle No. 1:

<u>Principle No. 2</u> – Employers should provide timely and sufficient notice of what they claim as their trade secrets, the policies and procedures to be followed by employees to protect those trade secrets, and any restrictions the employers intend to impose on the future mobility of their prospective and current employees.

Both parties, but especially employers, should provide notice to the other about the scope and nature of any trade secret that impacts the competing interests of the employers and the employees. For example, as noted above and explained in greater detail below, an employer's use of agreements that include restrictions that may affect an employee's privacy or mobility should be disclosed in a manner that provides an employee with timely and sufficient notice of those restrictions.

Employers should provide clarity about what information it considers to be its trade secret. Whether in the form of identification of what is a trade secret or communication about any restrictions or expectations on employees with respect to trade secrets, employers should attempt to provide adequate notice at each stage of the employment life cycle to their employees so they can conform their conduct to those expectations.

Finally, employers should be cognizant of balancing their interest in protecting trade secrets with the potentially competing interests of their employees.

While employers should take the lead in communicating their trade secret policies and procedures to their employees, employees should be expected to cooperate in those efforts (e.g., by attending

training sessions offered by employers, and disclosing the existence of prior work that might compromise their ability to do their job). Employees should not ignore their former employers' trade secret interests or impede their efforts to protect them.

Principle No. 3 – Employees and new employers should take into account the legitimate interests of former employers in their trade secrets, and employees and new employers should take reasonable steps to mitigate against the risks of misappropriation of the former employers' trade secrets.

When employees leave their current employers to work for a competitor, it can be a combustible situation. Fears and tensions can be ameliorated, at least in part, where both the employees and new employers demonstrate proper respect for legitimate concerns that the former employers may have regarding the protection of their trade secrets. To help address those concerns, employees should cooperate with reasonable exit interviews, coordinate with their former employers concerning the return of any company electronic files and other property that may remain in their possession at termination, and not misuse company trade secrets in their new employment. Hiring employers should have sound recruiting and interview practices to screen candidates and protect the company from potential trade secret issues resulting from new hires and their retention, use, or disclosure of their former employer's documents. Once appropriate vetting of candidates has occurred and offers have been extended and accepted, hiring employers should, in consultation with affected employees, consider (if possible and practical) placing their new hires in roles that would not benefit from the trade secrets of their former employers. The hiring employers also should articulate to their new hires the requirement that they not misappropriate any information of their former employers.

Principle No. 4 – In response to an impending employee departure, the employer should identify, address, and communicate as appropriate legitimate concerns about the departing employee's compliance with their continuing obligation to protect the employers' trade secrets.

Employers should consider communicating to departing employees their concerns that employees have misappropriated or will misappropriate the company's trade secrets to the benefit of their new employers and solicit a dialogue to resolve those concerns. On the other hand, where appropriate, employers may wish to monitor the situation for evidence of misappropriation (or threatened misappropriation) before confronting employees or beginning litigation. And, of course, some circumstances may call for immediate filing of a trade secret misappropriation lawsuit seeking provisional relief.

In addition to or as a part of exit interviews, employers often use reminder letters and certifications to obtain reasonable assurances from departing employees that they will honor their post-termination obligations. Tensions can quickly escalate where such efforts are ignored, as this may suggest (or be interpreted by the employer to suggest) that the employer should be concerned about the retention of or misuse of company property by the departing employee. This is particularly true when the departing employee will be performing similar work for competitors and in other situations that may appear to compromise the company's interests. Employers should use a tailored approach to protect their trade secrets, including, where practicable, by focusing on their legitimate concerns and obtaining reasonable assurances in order to avoid litigation.

This *Commentary* addresses all three stages of the employment life cycle—the recruiting and onboarding period, the ongoing employment period, and the offboarding and postemployment period—and applies the four Principles introduced above to guide employers how not to overreach or under-reach in protecting trade secrets.

II. Recruiting and Onboarding Period

Principle No. 1, as presented above, states:

> There is an inherent tension between an employer's interest in protecting its trade secrets and an employee's interest in engaging in future employment. Employers should tailor their policies and procedures to guard against the risk of unlawful use or disclosure of their trade secrets, while avoiding inappropriately restricting their former employees' application of their general knowledge, skill, and experience in their next employment.

Applying Principle No. 1 to the recruiting and onboarding period, new employers should conduct their hiring process and design employment policies both to protect company trade secrets and to reduce the risk of misappropriation of former employers' trade secrets. Any such trade secret protection policy should, however, be tailored and avoid unnecessarily restricting the employees' interests in future employment and future application of their general knowledge, skill, and expertise.

A. RECRUITING NEW EMPLOYEES AND ATTEMPTING TO REDUCE THE RISK OF TRADE SECRET MISAPPROPRIATION

1. Recruiting when trade secrets are potentially an issue

When companies begin recruiting, they must assess the risks of hiring competitors' employees.[8] While employee mobility may be valuable and an important part of a functioning economy, it puts the hiring employer and potential employee in a potentially tricky situation, as a competitor's

[8] This *Commentary* focuses on the employer-employee relationship and employment lifecycle. However, many of the issues that arise in that context can be the same or similar to the issues arising in the consultant and contractor context. For example, the Defend Trade Secrets Act (DTSA) applies to employees and independent contractors alike, meaning that consultants and contractors must abide by confidentiality restrictions and are afforded the same whistleblower protection as regular employees. In contrast, consultants and contractors often differ from employees in that they may simultaneously work for multiple companies, and could even work for two competing companies at the same time, potentially posing risk to each company's trade secrets. Further, the issue of knowledge retained in an individual's unaided memory that is discrete from any trade secrets that he or she may have been exposed to while working for a company is often addressed differently based on the relationship of the parties. Given the many specific issues that can arise and the considerations that must go into their evaluation, which can be quite different in the different contexts, consultants and contractors are outside the scope of this specific *Commentary*.

Employers sometimes use certain consultants and contractors that have the same "look and feel" as employees (even though for various business reasons they may not be classified as employees) and only work for that employer or contracting party during the consultancy or contract relationship. In those instances, the general protection strategies and approaches discussed in this *Commentary* concerning the employment relationship (e.g., recruiting, onboarding, training, exit interviews) are more directly applicable. However, even in those specific situations, companies must be vigilant concerning trade secret exposure in each of the recruiting, onboarding, training, working, and departing procedures, particularly since the consultant or contractor (in contrast to an employee) typically does not have a duty of loyalty, may not be subject to or familiar with the company's agreements and policies to protect confidentiality, and may have access to and store the company's data on the consultant's or contractor's devices or accounts, rather than the company's equipment or systems. Additionally, the company may be exposed at the time of the contractor's termination because it may not have the same ability to conduct exit interviews and obtain removal of company data from the contractor's devices or accounts. Carefully contracting with such contractors or consultants to provide protection rights is essential to ensure that company trade secrets are protected in these scenarios.

employee may come with knowledge of the competitor's trade secrets. To recruit a competitor's employees in a way that does not lead to the use or disclosure of the former employer's trade secrets is critical for all involved: the former employer, the employee, and the new employer (i.e., the former employer benefits in that the measures may reduce the risk of misappropriation of its trade secrets; the new employer and employee benefit in that the measures may reduce the risk that the former employer will assert misappropriation claims against them).

As stated above in Principle No. 3:

> Employees and new employers should take into account the legitimate interests of former employers in their trade secrets, and employees and new employers should take reasonable steps to mitigate against the risks of misappropriation of the former employers' trade secrets.

Hiring employers should evaluate risk of exposure to trade secrets when hiring from competitors and implement appropriate measures to guard against improper acquisition of trade secrets, while balancing their own right to hire and the employee's right to mobility. Prudent management will impose rigorous discipline on the recruiting effort, both to erect guardrails against cavalier behavior and to help drive the message to the workforce that lawful and ethical behavior is critical to mitigating risks.

a. Internal recruiting

Internal recruiting aided by a skilled human resources (HR) department is a useful way to reduce the risk of misappropriation of former employers' trade secrets. Existing employees are often a source of referrals of prospective employees. Nevertheless, employees may still be bound by continuing obligations to former employers, including nondisclosure obligations (contractual and under applicable law), noncompetition restrictions, and no-recruit commitments (i.e., agreements not to solicit former colleagues from their former employers). If this is the case, then taking a new job at the same company or asking former coworkers to come work with them may violate these postemployment obligations. To manage this scenario, employers should typically review potentially applicable ongoing obligations owed to former employers to understand if the employee's moving to the proposed new position or recruitment efforts would violate any continuing obligations, and caution the employee that nothing should be construed as an invitation to disclose former employers' (or others') trade secrets, and that the company requires the employees not to disclose any such information to the company.

Recruiters should be presented with an unambiguous message to avoid contamination with a competitor's data. Depending on the sensitivity of the hire, this may be the primary imperative for those doing the recruiting, and they need to have those concerns top of mind. This may translate into specific guidelines and checklists for promoting the position and for speaking with candidates.

b. Outsourced recruiting

The use of outside recruiters, recruiting websites, and services like LinkedIn can be helpful for companies, because recruiting firms are able to integrate sourcing, recruiting, hiring, and, in some instances, even onboarding. With some third-party recruiters, however, employers may be taken out of the process altogether, which makes it difficult to assess the prospective employees before they

show up for the interview. Because of this disconnect between the employer and the candidate, it can be difficult to discern whether the candidate possesses another employer's trade secrets or what ongoing obligations the candidate owes to current or former employers. Employers should use special care when using outside recruiters to hire a competitor's employees and make sure that trade secret exposure issues are appropriately considered and addressed. Employers should require their outside recruiters to ask candidates to identify any limitations on their ability to take on employment and any obligations to former (or soon to be former) employers that survive termination of employment, including but not limited to restrictive covenant agreements, and to confirm that, if hired, they are able to take the position and perform the related responsibilities without violating any obligations to others.

c. Drafting the job description

Both HR and business units typically play a role in drafting a job description. When drafting a job description, it is important to include both specific and general language with trade secret protection strategies in mind. The description should be specific as to exactly what the employer is looking for. For example, "we are looking for someone with experience" or "we are looking for an individual that does X." However, the job description should also be written generally enough to avoid revealing any trade secrets. It is important to note that during litigation, the job description may be offered as evidence to support a misappropriation claim (e.g., if it arguably (a) demonstrates the similarity in roles for a noncompete claim or (b) suggests "inevitability" of use of trade secrets or threatened misappropriation). Therefore, a job description, should be carefully crafted with potential misappropriation claims in mind when potentially hiring from a competitor (e.g., reflect the company's requirements that, if hired, the candidate not misappropriate any trade secrets and that the candidate be able to perform the job responsibilities without misappropriating any trade secrets). As the candidate proceeds in the hiring process, the job description may need to be modified to reflect the particular skills the employee brings and any restrictions to which the employee may be subject by law or by contract with a former employer. Any such modifications to the job description should be clearly documented to prevent confusion.

2. Risks of restrictive covenants, confidentiality agreements, inevitable disclosure, and actual or threatened trade secret misappropriation

An employer will want to find out as much as it can concerning a prospective employee's fit for the position, while taking care not to ask the candidate to provide any nonpublic information related to a prior employer. This process should begin with the collection and review of documents reflecting nonconfidential aspects of the candidate's prior work history. Prospective employers should typically consider whether to request the following types of documents from the candidate, to the extent they are potentially implicated by the anticipated position:

- Any written employment and other agreements (e.g., offer letters, stock option agreements and restricted stock unit agreements) containing a noncompetition, nonsolicitation, or confidentiality agreement;[9]

[9] Depending on the jurisdiction, such agreements may be enforceable in whole or part or not at all. The propriety of their use and assessment of their enforceability is beyond the scope of this *Commentary*. Because employees may not consider offer letters containing terms of employment or deferred compensation agreements to contain restrictions on employment, employers should counsel them to think broadly in assessing whether they may have applicable

- Any invention disclosure or assignment agreement;
- Any separation or severance agreement with restrictive covenants or confidentiality provisions; and
- Any patents and published patent applications that identify the prospective employee as an inventor.

As a general matter, employers should ask about obligations that may be implicated as a result of the employee's anticipated role; for example, a nondisclosure or noncompete agreement if restrictions therein may preclude employees from engaging in certain anticipated activities at their new employment. Accordingly, assuming there are no lawful confidentiality restrictions prohibiting an employee from sharing those documents, the employee should typically provide them.

If the employee's role might potentially violate a noncompetition obligation, both the employee and the new employer will want to understand the enforceability and parameters of the restriction. The employer may want to learn additional information—for example, how long did the employee work for the prior employer? What were the circumstances under which the employee was asked to sign the agreement? Was any consideration provided for the agreement? Did the employee's role change after signing the agreement? If the new employee joined from former employment with a competitor, the current employer's instructions for complying with the new employee's obligations to the former employer may be relevant. With that understanding, each party can determine for itself whether the anticipated role creates potential exposure and whether the role can and should be modified in such a way as to limit the potential fallout, such as by putting the employee in a role that does not expose the former employer's trade secrets to potential misuse (even if accidental).

Responsible companies will want to balance their own interests with the interests of their employees and the interests of the former employers in protecting trade secrets and contractual relations.

3. Conducting interviews

a. The risks of disclosure and solicitation of disclosure of trade secrets during interviews

Employers and employees must both take precautions during the interview process to prevent the disclosure of any trade secrets. The employer should avoid disclosing its own trade secrets to a candidate, and should avoid asking questions that are likely to prompt the candidate to disclose a third party's trade secrets. Similarly, candidates should avoid disclosing another's trade secrets to the employer. Each should also attempt to begin to gauge the trustworthiness of the other before the interview even starts.

For example, when selecting applicants to interview, an employer should consider whether the candidate's work history suggests any concerns.[10] It should be especially careful when recruiting

agreements. Long-term employees should think back to when they joined their current employer to ensure that they have a complete perspective on their restrictions.

[10] Potential risks to the would-be-employer from mining the Internet or social media for information about the employee or candidate is beyond the scope of this *Commentary*.

from competitors, as there is a risk that the candidate will disclose the competitor's trade secrets or that the candidate will attempt to relay the prospective employer's trade secrets back to the competitor. Potential red flags may include frequent job changes, a resumé disclosing information that appears too specific and is perhaps confidential to former employers, and prior restrictive covenant or unfair competition litigation.[11]

In addition, employers should never attempt to solicit the disclosure of trade secrets from the candidates they interview, and candidates should not disclose such information. Accordingly, employers should not ask candidates specific questions about their prior employment that may reveal trade secrets and should caution candidates that they should not reveal trade secrets in the course of the interview. Examples could include seeking the identity of particular customers whose identities are not readily in the public domain, and nonpublic information on current products or processes on which the employee is working. Rather, employers should talk about the candidates' talents, skills, general experience, and qualifications without seeking company-specific information.

Prudent employers use standardized protocols and forms to communicate specifically to candidates that they are not to reveal any trade secrets, both to prevent exposure and to create a record. Employers should create a system for communicating with potential recruits that consistently reinforces the company's respect for others' trade secrets.

b. Plan ahead for the interview

Employers should have well-defined plans concerning how to conduct interviews of candidates, particularly from competitors or otherwise where trade secrets could potentially be disclosed. Recruiters, human resources, and all businesspeople involved in the interview process should remember to discuss only the candidates' skills and talents, not their employers' customers or trade secrets. Those involved in interviewing all need to be trained to radiate respect for others' intellectual property and to avoid asking questions that might lead to inappropriate disclosures. In the same vein, they should receive proper training concerning not disclosing the company's own trade secrets.

Human resources professionals also may choose to establish guidelines or criteria for topics that business and segment leaders should avoid during the interview process. Human resources and business teams looking to hire should discuss these guidelines and appropriate areas of inquiry during the recruiting process and prior to the interview.

c. Requiring candidates to certify they will not disclose trade secrets during the interview

Especially where there is a particular risk of the disclosure of trade secrets or a restrictive covenant dispute, potential employers may wish to ask candidates to certify in writing that they do not believe that performance of those job duties would entail any reliance upon their former employers' trade secrets. If this approach is taken, candidates should be provided a detailed description of their proposed job duties before being asked to sign the certification. The certification should also

[11] To be clear, each of these is simply cause for inquiry, not a cause for immediate disqualification.

indicate that the candidate will not disclose any trade secrets during the application process and any interviews.

d. Training of businesspeople participating in the interview process

The businesspeople involved in the interview process should be trained to control the interview and put the candidate at ease. They should discuss in general terms the nature of the position for which the candidate is being considered, the company's expectations for employment, and ask only for a "yes" or "no" answer concerning whether the candidate has exposure to potential trade secrets of a prior employer or a third party that would be relevant to the candidate's performance of the proposed job. If the answer is "yes," they should ask the candidate (1) whether, based on the company's description of its job opening, the candidate can perform the job without—knowingly or unconsciously—using or disclosing what the prior employer is likely to claim as its trade secrets, and (2) if the candidate will agree to take care that no such trade secrets are used or disclosed by him or her during employment. If the candidate cannot provide those assurances, the company should reconsider proceeding any further with the candidate or consider whether modification of the job is feasible and appropriate.

e. Limiting facility access and notetaking during interviews

Candidates should have limited access to facilities before, during, and after an interview to reduce the risk that the candidate is exposed to any trade secrets. Additionally, if the candidate takes notes during the interview, he or she should avoid taking notes of any potential trade secrets. Similarly, the interviewer should not only avoid providing any such information, but should ensure that the candidate's notes do not contain any.

f. The risks of discussing projects and customers

When discussing projects and customers, disclosure should be limited, with discussion centering on generalized knowledge and not customer specifics. Typically, certain types of customer information are off limits, such as profitability, margins, order history, and ongoing projects. Other types of information, such as research and development, strategic plans, and future plans, are similarly off limits. Exceptions to this general rule may exist where, for example, the information is in the public domain or otherwise known in the industry to both potential employers and candidates.

B. EXTENDING AND ACCEPTING THE OFFER

1. Review of applicable agreements before extending the offer

<u>Guideline No. 1</u> – Before an offer of employment is made, the employer and candidate should make reasonable efforts to identify and evaluate the candidate's existing agreements that may impose obligations that affect the candidate's ability to fulfill the responsibilities of the proposed position with the employer. For executives or other sensitive hires, it may be advisable for the candidate to obtain independent legal advice concerning the candidate's continuing obligations under such agreements.

It is sensible for the hiring employer to understand what limitations the candidate may have working for the company prior to extending an offer. Employers should avoid scenarios where they have extended offers and employees have accepted such offers and tendered resignations without disclosure, consideration, or evaluation of the candidate's contractual restrictions and obligations with respect to the former employers' trade secrets.

In-house counsel or outside counsel should generally be consulted concerning the review of applicable agreements.[12] They may evaluate the restrictive covenants to see if they are enforceable. If they are, the company should assess to what extent employment is possible notwithstanding the restrictions. For example, depending on the restrictions, it may be possible to arrange for engineers to take on a different type of project or to assign sales personnel to operate in a different geographic area or market segment involving different customers. C-suite executives may not be able to take on a directly competitive position for a period of time after termination if doing so is likely to result in disclosure of trade secret information. If the officer's position is managerial rather than operational, however, it may be possible to tailor an appropriate position. Counsel, human resources, and the appropriate businesspeople should work together to identify the contractual obligations and the practical risk and implement safeguards to reduce the risk. In some cases, the hiring company may conclude that it is appropriate to work with the employee to challenge particular contractual restrictions.

Before extending an offer, companies should take into consideration the specific responsibilities of the position so that potential violations are avoided before employment starts. As the interviewing process proceeds, any restrictions the new employer concludes are advisable should, where possible, be communicated to the employee before acceptance of the offer. For example, candidates for sales positions should not be told only vaguely about the type of customers to whom they will be selling, only to find out later that they have to reach out to customers prohibited by their obligations to their former employer or that, because they will not be servicing particular customers, their commission-based compensation will be lower than anticipated.[13] Ideally, they will have a clear understanding of their assigned territories and clear expectations concerning their activity with regard to accounts they serviced for their former employer. Neither the new employer nor the new employee should want to be complicit in misappropriation.

Further, employees should not be asked to move outside their stated job description without first carefully considering the impact of any restrictive covenant. In crafting an appropriate role, careful consideration should be given to putting the prospective employee in a position to succeed without unnecessary encumbrance, but at the same time the new employer should be sensitive to the risk of misappropriation.[14] Employers who extend offers based upon securing customers of a competitor or

---

12 While recruiters may offer to provide this service, they may have a self-interest in the conclusion. Most organizations will prefer to evaluate enforceability themselves.

13 As already noted, however, the new employer will need to balance the need to be clear about the duties of the new position against the need to be circumspect about disclosing its own trade secrets to a candidate who is not yet—and may not become—an employee.

14 Some prudent employers will consider erecting walls around sensitive new hires where they are blocked from meetings, discussions, and information concerning customers or projects in those instances where there are concerns about improper disclosure of trade secrets. *See* Int'l Bus. Machs. Corp. v. Visentin, No. 11 Civ. 399 (LAP), 2011 WL 672025 (S.D.N.Y. Feb. 16, 2011); Amazon v. Powers, No. C12–1911RAJ, 2012 WL 6726538 (W.D. Wash. Dec. 27, 2012).

a competitor's technology put themselves at enhanced risk, particularly if the competitor has a protectable customer list or an enforceable noncompetition or nonsolicitation agreement.

2. Disclosing acceptance of a job offer to former employers

When employees transition to a new job, their goal should be to minimize harm to their former employers through steps such as giving prompt notice of acceptance of a job offer and continuing to abide by the former employers' confidentiality, noncompetition, and nonsolicitation agreements to the extent that they are lawful.

As a general rule, employees should be transparent about their plans and comply with any requirements to disclose their planned new employment. Accordingly, if asked (or required by contract or otherwise) to disclose who they are transitioning to work for, employees should answer truthfully; failure to do so (in addition to a breach of any applicable contractual requirements) will raise suspicions and potentially create problems unnecessarily.[15] Employees may conclude that they do not want to disclose the full details about their new positions to their current employers and may not be required to do so by contract or otherwise. But employees should not lie—as this will be pointed to as evidence of lack of trustworthiness in any future litigation.[16]

The new employer should encourage the employee to make a smooth transition and to provide necessary assistance to his or her former employer in transitioning. The new employer should, however, be wary of a start date that occurs any material time after acceptance of the offer. It should counsel the employee not to share trade secrets or to let up in his or her work for the soon-to-be former employer during the interval between the offer acceptance and the employee's last day with the former employer. In other words, the new employer should do what it can to ensure that the new employee is not acting as though he or she has already joined the new team before he or she has left the old one.

---

[15] Two cases are particularly instructive about the issues that can arise when employees fail to disclose—or misrepresent—their acceptance of a competitor's offer.

In *Bimbo Bakeries USA, Inc. v. Botticella*, 613 F.3d 102 (3d Cir. 2010), the defendant accepted employment with Interstate Brands Corporation on October 15, 2009, but did not give notice to his then-present employer, Bimbo Bakeries, until January 4, 2010. And even then, he did not disclose that he was going to work for Bimbo Bakeries' competitor until January 13, 2010, only two days before his resignation date. Due in part to the defendant's failure to alert Bimbo Bakeries of his new employment, he was able to attend a number of strategic meetings, in which he admittedly felt conflicted (a problem he dealt with by trying to forget what he had learned or not pay attention) and load his personal computer with confidential information, using at least three external storage devices. Ultimately, Bimbo Bakeries succeeded in obtaining a preliminary injunction against the former employee, who did not have a noncompete agreement, preventing him from working for the competitor.

In *PepsiCo, Inc., v. Redmond*, 54 F.3d 1262 (7th Cir. 1995), although the defendant accepted an offer with the Quaker Oats Company, a direct competitor of his then-employer PepsiCo, he told PepsiCo that he had received an offer from Quaker, but that he had not yet accepted it. As a result, the defendant continued making visits to PepsiCo customers, while having secretly accepted employment with Quaker. Partly in relying on this lack of candor, PepsiCo succeeded in obtaining a preliminary injunction against the defendant.

[16] Employees do not generally commit a tort by failing to disclose that they are thinking of leaving or that they are interviewing.

3. Reducing the risks of retaining potential trade secret information of former employers

An employee should ensure that he or she does not take or retain any trade secrets (or other property) of the prior employer and should ordinarily coordinate with the prior employer to ensure that this does not happen. The employee should typically notify the soon-to-be former employer if he or she has any company data or trade secret information on personal devices and accounts.[17] The soon-to-be prior employer should work with the employee to appropriately lock down the information. In some instances, the former employer may instruct the employee to simply delete the materials. In other instances, a computer forensic examiner, engaged by the former employer or by the hiring employer, may be needed to ensure the full return or deletion of the material as well to preserve it at various stages in a forensically defensible manner as appropriate under the specific circumstances.[18]

Pursuant to Principle No. 3 above, the new employer will typically want a new employee to represent in writing that they did not retain or bring to the new company, and will not use at the new company, any trade secrets or other property of the prior employer and that they will otherwise abide by all lawful agreements of the former employer. The hiring employer should emphasize that this requirement is real and not simply empty "boilerplate" language. The agreement between the new employer and employee may also provide that the company may terminate employment and seek damages for unlawful breaches and failure to disclose prior agreements.

4. Tailoring employees' roles to mitigate trade secret risks

When job applicants are uncertain whether they can provide written assurances that the performance of their new job duties will not lead to the use or disclosure of a former employer's trade secrets, or where the risk of litigation seems high in view of the potential overlap and the work to be assigned to the new employee, employers might want to refer the matter to outside counsel for further investigation.[19] Outside counsel may be able to discuss the scope of the applicant's job duties for the former employer while avoiding disclosure of the former employer's trade secrets to the new employer; engagement letters with such outside counsel should insist that the former employer's trade secrets not be shared with the hiring employer. Understanding the scope and type of work is important because it will inform whether there is substantial or little risk of trade secret misappropriation—even if the two companies are offering some competitive products or services. The use of outside counsel can be invaluable in evaluating any legal risk and in developing appropriate strategies for mitigating the risk. Moreover, following such procedures may reduce the

[17] There may, however, be instances in which an employee should consult with counsel prior to communicating with a soon-to-be former employer. For example, sometimes employees believe that it is permissible to take information with them to a new employer, only to later learn that such conduct is not appropriate. In such an instance, proper advice of counsel separate from the hiring organization may be needed to evaluate the facts and determine the best approach to handling the misstep.

[18] If this is done, steps must be taken to ensure that the new employer does not receive a copy of any company materials that are preserved.

[19] Depending upon the factual circumstances, separate outside counsel for the employee alone may be advisable.

risk of a willfulness finding and concomitant enhancement of damages and attorney's fees even if a trade secret misappropriation does occur.[20]

To the extent that there appears to be a reasonable likelihood that a new employee could use or disclose a former employer's trade secrets, the employee and new employer (and counsel) should attempt to lower that risk. Such practical mechanisms may include:

- being clear that an employee must arrive "clean," with none of his or her former employer's information with him or her, at his or her home, or on his or her personal devices or cloud storage, and that violation of that policy may lead to termination;

- having the employee sign an agreement that includes a promise to respect the intellectual property rights of others and that discusses how the new employee will be expected to handle the transition and how he or she will be expected to interact with his or her new colleagues—with reinforcement both verbally and in writing that the hiring company is serious about these provisions and intends that they be followed;

- creating a point of contact to answer questions or concerns and ensure that the employee receives meaningful training on how the company handles its own and others' trade secrets;

- walling the employee off from certain projects and/or customers that present particular risk of misappropriation or perceived misappropriation, and reflecting these limitations on employment in the offer letter or in subsequent memos in writing to avoid uncertainty;

- utilizing a clean room for significant work posing particular risk performed by the employee and which is vetted by outside counsel prior to use in any company projects;

- training and communicating with other employees about areas of inquiry that are off-limits with the employee; and

- where warranted, periodically reviewing and analyzing the employee's email and computer activities through smart forensic searches in an attempt to ensure no contamination. For example, if an employee's newly issued computer is populated by the employee with multiple gigabytes of data in the employee's first week of work, further investigation will likely be warranted. Similarly, some software development organizations will not "commit" code from a new employee to the corporate "code bank" without careful review to assess its origin.

[20] *See* 18 U.S.C. § 1836(b)(3); Uniform Trade Secrets Act, §§ 3(b) & 4.

Further, employers may consider providing new employees some discretion to decline work assignments if they perceive a legitimate risk of use or disclosure of their former employers' trade secrets but are not at liberty to explain why without revealing the actual secrets. Outside counsel can be consulted to assist with this process.

C. ONBOARDING—TRADE SECRET RELATED AGREEMENTS

1. Confidentiality agreements

Employers should include in their employment agreements an acknowledgment by new employees that the new employers have valuable trade secrets to which the employee will or may have access. The agreement should put employees on general notice of what kind of information is included and that this notice should be reinforced throughout the relationship by training. It should also include a covenant by employees not to improperly access, use, disclose, or retain such information outside of or following employment. These agreements are a common vehicle for companies to protect their trade secrets. Depending on the jurisdiction, such an agreement may require an outside time limit as it applies to confidential information (as opposed to trade secrets) and may be invalidated if too broad in the scope of what it purports to claim is confidential. Such a provision may be standalone or included in a broader employment agreement or other similar agreement.

Confidentiality agreements serve multiple important purposes, including putting employees on notice that the company has information that may be confidential in general, and identifying for the employee particular types of information that the company considers its trade secrets. Also, nondisclosure agreements are an important building block of the company's overall efforts to take (and ability to demonstrate that it has taken) reasonable measures to protect its information. They also may provide a breach-of-contract claim for the unauthorized use, disclosure, or taking of company information, in addition to a trade secret misappropriation claim.

a. DTSA's whistleblower language

The Defend Trade Secrets Act (DTSA) provides that employers "shall" include a notice of whistleblower immunity in any contracts with employees, contractors, or consultants that include provisions restricting the use or disclosure of trade secrets. Absent providing such notice, employers cannot recover attorneys' fees or enhanced exemplary damages. The notice must inform employees that they are permitted to disclose a trade secret in confidence to a federal, state, or local government official, or to an attorney, when such disclosure is made to investigate or report a suspected violation of law, or in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal. Additionally, the notice, which can be expressed in general, easy-to-understand terms, should advise that individuals suing their employers for retaliation based on the reporting of a suspected violation of law may disclose a trade secret to their attorneys and use the trade secret information in the court proceeding, so long as any document containing the trade secret is filed under seal and the individual does not disclose the trade secret except pursuant to court order. The required disclosures can, in the alternative, be contained in a nondisclosure agreement or other appropriate company policy or handbook, including cross-referencing the DTSA's immunity language in the company's general whistleblower procedures.

b. Examples of information pertinent to the company that the company identifies as a trade secret

Agreements that protect confidential information often contain lengthy, boilerplate definitions of confidential information. For many businesses, the general categories of confidential information are common and can include customer lists, formulas, patterns, compilations, programs, devices, methods, techniques, and processes. Despite some areas of commonality, employers should consider tailoring appropriate definitions to particularly valuable or unique categories of information so there is no ambiguity about what the company deems confidential and so the agreement does not sweep in nonconfidential information. From the employee's perspective, it is essential that employers provide descriptions and examples of protectable information that are understandable, identifiable, and relevant to their businesses. Employers that overreach and fail to provide employees with this basic understanding run the risk that their employees will not sufficiently understand their obligations or that a court may refuse to enforce the nondisclosure obligation.[21] Employers should also be aware of not imposing obligations of specifically marking information as confidential in their agreements if they are not prepared to mark all such information. Courts have refused to protect alleged trade secrets where companies have not followed their self-imposed identification requirements in their nondisclosure agreements.[22]

c. Do not overcommit, and do enforce

As a general matter, companies should enforce their policies and agreements. If the company as a whole does not follow its own policies, there will be little incentive for its employees to follow them. This then heightens the risk that an employee will breach his duty of confidentiality, as the employee may view the confidentiality agreement as simply a suggestion rather than an obligation. Moreover, a routine failure to enforce may be argued by other employees as a failure to take reasonable steps to preserve the confidentiality of the information, thus undermining the ability of the employer to prove the information is in fact entitled to trade secret status. An employer's reasons for not enforcing particular restrictions should be a conscious and considered decision, not a careless omission.

2. Noncompetition agreements

In addition to confidentiality agreements, noncompetition and related agreements[23] may be used in some states to protect trade secrets. These agreements have historically been governed by state law

---

[21] Failing to put employees on notice may be a failure to take reasonable measures to protect the information, especially if the information is not "intuitively" a trade secret. *See* Electrocraft v. Controlled Motion, 332 N.W.2d 890, 902 (Minn. 1983).

[22] Convolve, Inc. v. Compaq Computer Corp., No. 2012–1074, 527 Fed. Appx. 910 (Fed. Cir. Jul. 1, 2013); Abrasic 90 Inc. v. Weldcote Metals, Inc., 364 F. Supp. 3d 888 (N.D. Ill. 2019).

[23] Nonsolicitation of customers provisions are used in addition to or in lieu of noncompetition agreements by some employers in those states that permitted such clauses. Like noncompetition agreements, nonsolicitation provisions may be enforceable in some states as necessary to protect trade secrets. The enforceability of nonsolicitation provisions is beyond the scope of this *Commentary*.

on restrictive covenants,[24] though that may change in the future.[25] This *Commentary* does not advocate a particular position as to the propriety of such agreements; nevertheless, any understanding of the various tools used by employers to protect trade secrets must include a discussion of them.

Employee advocates often argue that noncompete agreements are unnecessary because they do not serve any legitimate business interest, and that they are contrary to the public interest because they stifle creativity, and economic development, and the fair exchange of information, as well as employee mobility. They view noncompete agreements as blunt instruments that are prone to abuse because of overly aggressive drafting and enforcement. They often point to California's general prohibition of employment noncompete agreements and to California's economic development and the success of the technology sector in the Silicon Valley to support their position. Others point out that the Silicon Valley success story is multifaceted. The dialogue around these issues has led several states to recently pass legislation or propose legislation to limit the use of certain types of noncompete agreements with some kinds of employees. The new laws typically prohibit the use of noncompete agreements with low-wage workers or limit the duration and scope of such agreements.

By contrast with noncompete agreements, confidentiality agreements generally do not inherently prevent employees from working for a competitor. Thus, it is left to the former employer to police the former employee's conduct (i.e., monitor for any use of its trade secrets), often without the tools necessary to do so fully (i.e., the former employer has limited ability to know what the employee is doing until, in the worst case, it is too late, and the former employee has used the information).

For example, one of the most nuanced areas in trade secret law is how to handle the fact that trade secrets can often be retained in a person's memory. As a general matter, the mere fact that information is lodged in someone's head does not strip it of its trade secret qualities or the available protections. But it may be particularly difficult to detect whether a former employee is using in a new position trade secrets that he or she retained in memory without needing to rely on the physical or electronic transfer of information. Noncompetition agreements, however, can—for a period of time—limit the scope of, or even prevent altogether, an employee's engagement with a prospective employer. Thus, one justification that has been offered for noncompetition agreements is that because misappropriation is often "behind-the-scenes" and, as a result, difficult for the former employer to detect, noncompete agreements provide readily detectable boundaries to prevent misappropriation by keeping the employee (and therefore the trade secrets known to the employee) out of the market altogether for a defined period.

---

[24] The law, advisability, and drafting of restrictive covenants varies widely by jurisdiction (by state in the United States and by country outside) and is outside the scope of this *Commentary*. However, a brief overview is provided because of the significant role these agreements often play in the protection of trade secrets. For more information about noncompete agreements generally, see Brian Malsberger, COVENANTS NOT TO COMPETE (Bloomberg Law 2018) (12th ed.). Several law firms track the developments in noncompetition law across the country and they can be located through a simple internet search.

[25] Since 2015, bills have been presented in Congress to ban or regulate the use of noncompete agreements. And, starting in 2019, the FTC has been considering whether its rulemaking authority permits it to regulate noncompete agreements, and if so, to what extent. Both Congress and the FTC have been considering complete bans or less comprehensive regulations such as banning the use of noncompete agreeements, requiring advance notice to be provided to employees who will be required to sign a noncompete agreement, and preventing courts from modifying unnecessarily restrictive agreements.

Accordingly, noncompete agreements can offer the advantage of serving as a prophylactic tool for companies to prevent the circumstances in which trade secrets are likely to be put at risk—such as when an employee moves to a competitor in a role that threatens disclosure of the company's trade secrets—and thus may prevent misappropriation before it happens.[26] While state laws vary to some degree, the protection of trade secrets is recognized as a legitimate basis for the use of noncompete agreements in many states.[27]

Outside of California, Oklahoma, North Dakota, and to a large extent, the District of Columbia, noncompete agreements may be enforceable, but only if and to the extent they are "reasonable" and comply with any statutory or common law requirements of the relevant jurisdiction. Noncompetition agreements are generally disfavored in the law because they are restraints on trade, and as a result, unlike most contracts, they are reviewed by courts for reasonableness. In most states permitting noncompete agreements, courts generally balance the interests of the particular employee against the interests of the particular employer in the particular case. Consequently, under most applicable state laws, noncompete agreements must be reasonable in time (typically one to two years, depending on the state), space (the territory in which the employee is restricted), and scope (the nature of the work in which the employee is prohibited from engaging during the restricted period). A "reasonable" agreement typically limits the employee's right to engage in competitive activities only as far as necessary to protect a recognized legitimate business interest, chief among them, the protection of trade secrets. A noncompete agreement is typically found to be unreasonable if it is used solely to limit the employee's right to work for competitors and prevent "ordinary" competition, as distinguished from "unfair" competition.[28] These "general" principles are being evaluated and commented on by courts and legislatures regularly, however, and are evolving. It is advisable to routinely consult with counsel to keep up with recurring changes in this area.[29] The continued use of noncompete agreements by companies and appropriate limitations on such agreements, particularly their use with low wage employees, which is defined quite differently by a

---

[26] Trade secrets are not the only recognized protectable interest. Other well-recognized interests include the protection of customer goodwill developed by the company (through the work it pays its employees to perform). Indeed, goodwill is frequently the primary concern for companies managing departing sales team members. But other legitimate business interests exist, depending upon the particular state. For example, some states permit noncompete agreements to be used to ensure that investments in training, sharing of information, and innovation are protectable.

[27] Only three states ban employee noncompete agreements, and the District of Columbia has a near-ban: California (*see* Edwards v. Arthur Andersen LLP, 44 Cal.4th 937, 945 (2008)); North Dakota (*see* Werlinger v. Mut. Serv. Cas. Ins. Co., 496 N.W.2d 26 (N.D. 1993)); Oklahoma (*see* Brandon Kemp, *Noncompetes in Oklahoma Mergers and Acquisitions*, 88 Oklahoma Bar Journal 128, at n.2 (Jan. 21, 2017)); and the District of Columbia (Ban on Non-Compete Agreements Amendment Act of 2020, D.C. Law 23-209).

[28] As a general matter, to maximize the likelihood that a noncompete agreement will be found reasonable, the noncompete period should be only as long as is necessary to protect any trade secrets to which the employee had access, and should be limited to the geographic area in which the employee was involved and to the product or services on which the employee worked. Another factor that sometimes contributes to a finding of reasonableness is a provision obligating the employer to pay a base salary or other compensation to a departed employee during the noncompete period if the employer invokes the agreement to prevent a departing employee from accepting a specific job offer with a competitor.

[29] Employers doing business in multiple states and countries often prefer uniformity in their restrictive covenant agreements. While uniformity may be an ideal, it may not be possible due to various state law limitations on such covenants or limits on specifying outside forums or choice of law. *See, e.g.,* Cal. Business and Professions Code Section 16600; California Labor Code Section 925 (prohibiting out of state choice of law and forum provisions in employment agreements subject to certain exceptions).

number of states, remains a hot button issue that state and federal legislators and regulators continue to scrutinize.

Employers should timely disclose to candidates before they accept employment any requirement that they sign a noncompete agreement. For example, waiting to disclose a restrictive covenant until the first day of the employee's job, or perhaps even thereafter, even where legally permitted,[30] can have multiple adverse consequences, including decreasing morale.[31] And it is often the disgruntled employee who poses the biggest security risk to a company.

[30] Additionally, employees are often frustrated when they are asked to sign noncompetition agreements for the first time after they have been employed for a number of years. Depending upon the jurisdiction, some state laws require employers to provide additional consideration in such circumstances, whereas some states do not. Employers may consider providing consideration even where it may not be required.

[31] Indeed, some jurisdictions are now requiring that the employee be provided with notice of the noncompete agreement with the formal offer, or otherwise prior to commencement of employment. Those states are ME, MA, NH, OR, and WA, as well as the District of Columbia. Gauging from proposed legislation, this number is likely to increase.

III. The Ongoing Employment Period

The boundary between protectable information and employee general skill, knowledge, and experience is inherently ambiguous. Because employers usually are in a better position to determine what information they consider to be valuable, they should take the lead in defining what they believe to be the company's trade secrets. Therefore, to minimize misunderstanding and maximize alignment between employers and employees, employers should use opportunities throughout the ongoing employment period to train and educate their employees regarding the identification of what information or types of information they view as their trade secrets and what processes employees are to follow to protect them.

An employee's level of exposure to trade secrets may influence the degree of training and protection obligations imposed on the employee. C-suite executives and managers will typically have access to more trade secrets, and as leaders, should be expected to not only be familiar with company confidentiality policies and practices, but to consistently follow and be role models for other employees. Likewise, scientists and engineers engaged in research and development projects may have greater access to trade secrets. As employees remain with the organization and gains access to new types of information, further training is likely necessary so that all are on the same page regarding the information to be treated as confidential, how it should be treated, and how such information is and is not affected by developments in the industry.

Ultimately, managing trade secrets during the duration of the employment relationship should be part of an overall company trade secret protection program and the development of a company culture of respect for legitimate intellectual property rights.

A. IDENTIFICATION OF TRADE SECRETS BY THE EMPLOYER

Trade secrets come in a vast range of formats and types of business information. Their commercial value can also cover a wide range, from "bet the company" assets to information that a company would prefer not to lose but would not drive the company out of business if it was lost. And while some companies may elect to implement a program that catalogs their trade secrets, others may elect for myriad different reasons not to do so. This issue will be discussed in more detail in the forthcoming The Sedona Conference's *Commentary on the Governance and Management of Trade Secrets.*

There is a robust debate about the extent to which employers should implement a program identifying and cataloging its trade secrets. Nevertheless, there are multiple reasons that some degree of identification of trade secrets to employees benefits both the employer and the employees.

As stated above in Principle No. 2:

> Employers should provide timely and sufficient notice of what they claim as their trade secrets, the policies and procedures to be followed by employees to protect those trade secrets, and any restrictions the employers intend to impose on the future mobility of their prospective and current employees.

Given that employees are essential to the successful implementation of trade secret protection programs, employees need to have some level of understanding of what information qualifies for

that protection. And by providing some level of notice of information that employers consider to be their trade secrets,[32] that identification may promote a dialogue about whether certain information can be protected or whether there are potential disputes between employers and employees about the ownership of that information. Furthermore, courts have required employers to provide their employees with some level of notice of what the employer claims as its trade secrets.[33]

Guideline No. 2 – Employers should identify for their relevant employees the categories of information they consider to be trade secrets, and provide examples where practicable.

At a minimum, to the extent that employers expect their employees to implement programs protecting their trade secrets, employers should identify the categories of trade secrets that they expect them to protect. This should be provided in training and education, as described below.

Guideline No. 3 – In assessing and communicating to employees what information is to be protected as their trade secrets, employers should be mindful not to sweep in information that is not their trade secrets, including the information that is generally known or is part of the general skill, knowledge, and experience of their employees.

It may be advisable for the employer to use greater specificity in identifying its trade secrets for those employees who are tasked with research and development or involved in generating or creating information that the employer considers to be its trade secrets. While these employees can be expected to appreciate the value of that information, it may be prudent for the employer to ensure that they understand the information that they are working with and developing is proprietary, confidential, and the property of the employer. Employers and employees alike should be aware of the fact that there is often a "lag" in identifying new trade secret information that is being developed. An organization's trade secrets are typically not frozen in time. The fact that information developed five years into an employee's career with an organization is not identified as a trade secret in the initial onboarding materials does not mean that the employer cannot subsequently identify this information as a trade secret through training and exit proceedings. In turn, the fact that the employer properly identified information as a trade secret five years before does not mean that the information remains a trade secret now.

---

[32] The resources, size, and sophistication of the employer may impact the scope and level of the notice that may be provided. For example, it is reasonable to expect that a Fortune 500 company will be better equipped to develop standards and policies to provide that notice. Conversely, it may not be reasonable to expect a small startup to have the capability to develop those same standards and policies and provide the same degree of notice, although the smaller organization should also make efforts to inform the employee of its overall expectations.

[33] *See, e.g.,* Electrocraft v. Controlled Motion, 332 N.W.2d 890, 902 (Minn. 1983) (holding that because employer had not identified information that is not "intuitively" a trade secret has not protected it as such when sharing it with employees).

B. POLICIES AND PROCEDURES REGARDING TRADE SECRET INFORMATION DIRECTLY IMPACTING EMPLOYEES

The employer should develop and communicate to its employees policies that address company trade secret information. These policies serve many purposes, but they should strive to meet the following three guidelines:

Guideline No. 4 – Trade secret policies should provide notice to employees about the employer's expectations for protection, management, and use of trade secrets during the employment relationship and thereafter.

Guideline No. 5 – Trade secret policies should provide guidance to employees on what they should do, or whom they should consult, in the event that a question about the management, protection, or use of trade secrets may arise.

Guideline No. 6 – Trade secret policies should promote communication between the employer and its employees about the employer's intellectual property protection policies and procedures and should facilitate employee questions or considerations about them, both during and following employment.

The courts frequently consider confidentiality policies when examining whether an employer has taken reasonable measures to protect its trade secrets and to enforce trade secret interests against others who the employer believes misappropriated or threatens to misappropriate the employer's trade secrets.

Confidentiality policies can take many forms. Many employers use a "Code of Conduct" or similar approach to instill their policies as ethical principles that employees should follow. Others may focus on a comprehensive employee handbook to convey the information. Whatever their form, written policies may be an important first step in providing tangible guidance to employees on how to use, share, and manage trade secrets.

Several trade secret policies directly impact employees,[34] and as such merit heightened attention in their development, communication, and implementation, including:

1. Post-termination obligations

Trade secret protection programs should address obligations that employees have for the return and treatment of trade secret information when and after their employment relationship ends. These obligations, as documented in each employee's employment agreements and in any associated policies,[35] should be reinforced periodically and consistently throughout the ongoing employment period.

---

[34] For a broader discussion of other company policies that are part of or affect a company's trade secret protection program, *see* the forthcoming The Sedona Conference's *Commentary on the Governance and Management of Trade Secrets.*

[35] *See supra*, Sect. II.C. (Onboarding—Trade secret related agreements).

2. Treatment of former employers' trade secrets

The prohibition against using any trade secret information of former employers should be memorialized in each employment agreement, and employers should emphasize this throughout the employment period. Not only does this help mitigate against the risk of disputes or litigation with the former employers, but it further serves to reinforce the importance of protecting and respecting all trade secret information, including the employer's own trade secrets.

3. Bring-your-own-device (BYOD) policies

The use of personal devices for business purposes is fraught with the opportunity for inadvertent or intentional loss or misuse of trade secrets. Mitigating against this risk is further complicated by the fact that any BYOD policy implicates private information, photos, or other personal information on these devices owned by the employee. If a company elects to allow employees to perform work on employee-owned devices, these issues should be addressed in the employer's policies. The policy should clearly notify the employees participating in the BYOD program that the employer retains and reserves the right to access, monitor, and delete information from the employee-owned devices. The policy should describe the circumstances under which the employer can exercise those rights and the scope of those rights:

- To eliminate doubt and ensure all expectations are aligned, employers should make sure that they secure consent from their employees so that the employees clearly understand the rules, terms, and conditions that govern participation in the BYOD program. If there are noteworthy changes that are being made to the BYOD program, acknowledgements for those changes should be secured.

- If an employer intends to use any forms of monitoring, it should notify its employees of its right to monitor that activity at the outset of the employment relationship.

- Employers should also notify employees that the employee has reduced expectations of privacy in personal (not employer-owned) files.

For an indepth discussion on these issues, see *The Sedona Conference Commentary on BYOD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations*.[36]

4. Ability to work on side opportunities/projects

Some employees, particularly researchers, software coders, and engineers, may be interested in doing side work, moonlighting, and partnering with others in what they believe are opportunities unrelated to their employment. Employers may permit or even encourage them to take advantage of these opportunities for a variety of reasons, including opportunities to allow employees to earn other income or further develop skills that contribute to the employer's business.[37] However, these

[36] The Sedona Conference, *Commentary on BYOD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations* (May 2018), 19 Sedona Conf. J. 495 (2018).

[37] Restrictions on such opportunities may also be subject to developing state law. *See supra*, note 27.

opportunities are not without risk, as an employee may misuse or improperly share trade secrets in connection with those opportunities or find themselves in a position to potentially use that information to compete against an employer now or in the future, therefore creating a situation for a breach of any duties of loyalty that they may owe to their employer. Consequently, special care should be taken by employers in these situations to specify by policy and reinforce through communications the parameters of such outside consulting work to reduce the risk that trade secrets are misappropriated.

5. Ownership of intellectual property

Employers may (and often do) take a broad view of their ownership of the information that is generated over the course of the employment life cycle. But many employees bring certain information with them to their job and develop new skills and information while on the job. This information is frequently described as "general skill, knowledge, and experience," and it is a baseline expertise that a reasonably successful employee in that position and industry would be expected to have.[38] When those skills are brought to bear in the process of helping develop or create work product for the employer, there is potential for a dispute over whether the resulting information belongs to the employer or is properly accretive to the employee's general skill and knowledge, often turning on whether the product of information is something that a comparably placed and skilled employee would be able to develop elsewhere.

Courts have grappled with the proper line of demarcation between a trade secret and the general skill and knowledge/residual knowledge of an employee. Some of those cases have identified multiple factors as relevant in attempting to separate an employee's general skill, knowledge, and experience from the employer's trade secrets. These include:

- the degree of experience and expertise of the employee prior to joining the employer,
- the extent to which the claimed trade secrets consist of information or general principles already found in the public domain or known to others in the field,
- the extent to which the claimed trade secrets result from the application of basic problem-solving or knowledge within that industry,
- the extent to which the claimed trade secrets have been reduced to practice in the form of a functioning device or system,

[38] A related but very specific concept is "residual knowledge clauses" that one sees most often in contracts with consultants. These clauses typically provide in express language that the consultant is not permitted to use or disclose trade secrets of the engaging party, "provided, however, that this prohibition does not extend to information retained solely in the consultant's unaided memory without documentation" or the like. The rationale provided for using such contracts is that they bring knowledge gained from working from many clients and that the consultant wants to be able to use whatever she learned about, for example, optimizing particular software as long as the consultant does not bring or use particular code; otherwise, the consultant would have to charge a great deal more and the party engaging the consultant would not get the benefit of his or her work for other clients.

- the extent to which the information is carried in the employee's head as opposed to documented in files brought over from the former employer, and

- the degree to which that information is so integrated with the employee's overall employment experience that characterizing it as a trade secret of the former employer would deprive the employee of the ability to find commensurate employment elsewhere.[39]

While courts have not uniformly applied the same factors in their analysis, they have routinely held that the employer bears the burden of describing the information at issue specifically and establishing that the information at issue is not the general skill, knowledge, and experience of the employee. A full discussion of this complex issue is beyond the scope of this *Commentary*.[40]

Disputes over trade secret (and intellectual property in general) ownership often originate from employment policies imposed by the employer and from positions taken by the employer with respect to its claimed scope of its trade secrets. Many company employment policies and agreements include expansive claims to information generated or touched by its employees. A comprehensive discussion of such employment policies and agreements is beyond the scope of this *Commentary*, but some issues that merit discussion include:

a. Understanding the scope of the employee's general skill, knowledge, and experience

Employers should try to develop an understanding of what intellectual property rights employees owned prior to hire and are bringing into the employment relationship, so that the parties have a better understanding what rights the employees will retain or acquire, if any, during employment. This is typically done through a disclosure in the agreement identifying intellectual property that the employee owns or has an interest in prior to hire, including publicly registered intellectual property such as patents or copyrights. Such a provision is particularly important if the employee will be asked to integrate his or her intellectual property into the company's developments. However, the employer should not overreach by trying to use the employee's disclosure to assert a limit on the scope of the employee's general skill, knowledge, and experience.

b. Managing the risks of employee-owned intellectual property

---

39 *See* SI Handling Sys. v. Heisley, 753 F.2d 1244, 1264–65 (3rd Cir. 1985) (employee's ability and experience that led to developments does not belong to employer, including problem-solving and ability to identify mistakes to be avoided/negative trade secrets); Winston Research Corp. v. Minn. Mining & Mfg. Co, 350 F.2d 134, 144–145 (9th Cir. 1965) (finding that general approach of former employees was not a trade secret because it consisted of general engineering principles in the public domain with which they were previously familiar); Dynamics Rsch. Corp. v. Analytic Scis. Corp., 9 Mass. App. Ct. 254 (1980) (employee was hired by employer because he understood engineering concepts at issue).

40 For a discussion and additional context on the underlying issues, *see* The Sedona Conference, *Commentary on Equitable Remedies in Trade Secret Litigation* (May 2021 public comment version) Section V.A. (Evaluating the Movant's Likelihood of Success on the Merits), pp. 25–37 & nn. 94-157, *available at*: https://thesedonaconference.org/publication/Commentary_on_Equitable_Remedies_in_Trade_Secret_Litigation [hereinafter *Sedona WG12 Trade Secret Equitable Remedies Commentary*].

The existence of employee-owned intellectual property poses risks and challenges both during and after the period of the employee's employment.

One possible approach is for the employer to instruct the employee not to incorporate any preexisting work that the employee owns into any of the work that the employee creates for the employer, and if the employee does so, the employer will be provided with a royalty-free license to use it in the work that the employee created for that employer. This solution has the benefit of minimizing potential confusion about what is owned by the employer and also enables the employee, who is in the best position to identify and avoid using those inventions, to initiate any conversation about the relationship of that invention to the employer's intellectual property.

c. Providing a company resource for employees to address questions about intellectual property ownership

Employers should consider naming someone to address questions about intellectual property ownership to help prevent misunderstandings and disputes. An employee's decision not to call on such a resource during employment, however, should not be used to assert a limit on the scope of the employee's general skill, knowledge, and experience.

C. EMPLOYEE TRAINING ON TRADE SECRETS

In furtherance of Principle No. 2 above, employers should, at the inception of and throughout employment, provide employees with training that sufficiently identifies the categories of employers' trade secrets and the employers' expectations of employees concerning their creation of trade secrets, as well as access to and responsibility to protect such information.

Training and education are critical tools to ensure employee compliance with trade secret policies and procedures. Interactive training facilitates a greater shared understanding by employees and employers alike of the company's trade secret protection program.

Employees who understand what their employer considers to be its trade secrets, what they need to do to protect that information, and what the consequences are will generally be less likely to engage in conduct that puts that information at risk. Accordingly, in most instances, new employees—particularly those who may have little familiarity with trade secrets and their protection—should be provided with an appropriate level of proprietary rights protection training when they join the company, and as appropriate thereafter.[41]

Training should:

- provide a sufficiently detailed overview of the categories of information that the employer considers to be its trade secrets, including third-party information with which the employer and employee deal,

[41] A portion of this training could be in the form of a short video presentation on the employee's role in protecting the company's proprietary assets and trade secrets and can be shown to new employees as part of their orientation.

- emphasize the company's commitment to protecting its trade secrets (and other proprietary assets),
- explain the forms of protection relied upon by the company and applicable policies (see below), and
- describe the written materials and other company resources available to provide further guidance to the employee.

Employees need to understand the importance of dotting all the "i's" and crossing all the "t's" when it comes to trade secrets, including the trade secrets of a third party that the company is obligated to protect. Employees should understand that the third party's trade secret information is not to be used or disclosed without permission, even if they think the proposed activity is innocent or makes sense to them. They need to understand that they have an obligation to protect the third party's trade secret information from misappropriation, just as they have an obligation to protect their own employer's trade secret information.

Training tends to be more effective if it is tailored to particular employees' responsibilities. For example, a sales associate may not encounter the same types of situations involving trade secret disclosure risks that a research scientist typically would. Employees thus benefit from training hypotheticals that apply to their particular job responsibilities. However, there are administrative burdens that may be considered in deciding whether tailored training is realistic or cost efficient.

Training should focus on both sides of the trade secret continuum: safeguarding the employer's trade secrets and guarding against the improper receipt and use of the trade secrets of others, such as former employers. Practical training that provides tips on how to manage real-life situations can be particularly effective. For example, training on preventing use of former-employer information can include practical guidance on searching the public domain and documenting public sources of information when an employee is wondering whether he or she is able to use an item of information. Another practical training exercise could involve how to politely tell coworkers, customers, vendors and others that they might be inappropriately sharing information that might appear to be the trade secrets of others.

Employees should also understand that just because they *can* access another company's trade secret information does not mean that they *should*. Analogies can often help the employee understand: just because a person leaves the door to the house unlocked does not mean that you are free to walk in and take the television. Extending the analogy, just because someone else walked in and took the television and is offering to sell it does not mean employees can now legally help themselves to it.

Similarly, employees should understand that they have proper internal recourse if they are concerned that coworkers, consultants, vendors, or business partners may be engaged in conduct that has given, or could give, rise to misappropriation. To that end, employees should be aware of 1.) their primary point of contact for reporting purposes; 2.) what steps to take to document or memorialize the conduct in question; and 3.) the protection the company will afford them for identifying and reporting on such conduct.

In addition, employees should ensure that they honor any continuing confidentiality, noncompete, and nonsolicitation obligations owed to former employers. Human resources personnel should

follow up with the employees and the employees' managers to confirm that they all understand the scope of their restrictions and obligations.[42]

Finally, it is the reinforcement and implementation of those policies and procedures that is so critical in building a culture of confidentiality that ensures a workforce actually abides by and reinforces the need for confidentiality. Accordingly, while training and education are necessary, testing and consequences for the results of that testing are strongly encouraged.

- Identification of what is confidential and what to do about it: Does the employer truly assist the employee in understanding what should be treated as confidential and what do to about it? This is where including a "confidentiality" legend or designation, or encouraging employees to use those designations, may be useful but is not always possible or practical. Negotiating and executing general confidentiality agreements with vendors or third parties may be of limited value if the employees do not understand what to treat as confidential.

  And to what degree should an employer specifically identify the information it wishes to be treated as confidential? Given the number and potentially changing status of what may or may not be confidential, it may be best to rely on categorical designations (i.e., "highly confidential" v. "confidential") and provide examples of the types of information that fall within those categories.

- Frequency: Employers should provide periodic communications and training regarding its trade secret protection program. This may vary from company to company or industry to industry, but it should take place at some regular interval to ensure training is provided.

- Testing and Certification: Simply providing training and lectures may be insufficient. Confidentiality training should be accompanied by testing and, where possible, certifications that demonstrate core competency, understanding, and sufficient reinforcement. For performance reviews of certain employees, employers may consider including a metric assessing the employee's performance in complying with the company's trade secret protection program.

- Modes of training and education: Where possible, live training should be provided with real-world examples and situations to assist in reinforcing basic principles for protection of trade secrets. Employers should have online training and education available, but should couple that training with more rigorous testing to ensure compliance and retention.

- Consequences for failing to pass training: If there are no consequences, there will be diminished incentive to retain and use what is learned. Some

[42] HR personnel should be clear that they are not giving the employee any legal advice and that the employee is free to seek legal advice from his or her own attorney.

employers (in particular those who have gone through traumatic events involving their confidential information or suffered a severe breach) tie success in confidentiality testing and certifications to bonuses and other financial compensation.

- Training for all: Training should be required of C-suite and senior management, and should include managers (HR, legal, compliance, marketing, etc.) as well as the remainder of the workforce that has access to trade secrets.

IV. The Offboarding Period

Each time an employee leaves a company, there are risks for the former employer, employee, and new employer. Those risks vary significantly in many ways. For example, the risks posed by "rank-and-file" employees may be very different from the risks posed by research and development teams. In particular, rank-and-file employees typically do not have knowledge of critical trade secrets, whereas R&D teams typically do. Similarly, departing salespersons pose different challenges from departing C-level executives, although each may have significant potential ramifications for the employer.

Not every departure creates risks that warrant a response, much less the same level of response. Accordingly, as articulated in Principle No. 4:

> In response to an impending employee departure, the employer should identify, address, and communicate as appropriate legitimate concerns about the departing employee's compliance with their continuing obligation to protect the employers' trade secrets.

Many factors come into play in evaluating the risks, some of which deserve more attention and analysis than others. These factors include, but are not limited to, the level of the employee's position; the nature of the employee's work; the scope of the employee's access to information; the sensitivity of the information; the quality and duration of the employment relationship; the trustworthiness of the employee as assessed both during employment and in connection with the employee's departure; and the risks posed by the employee's role for the new company.

Further, while many of the factors focus on the employee and the nature of the particular employment relationship, external circumstances may play a role in the analysis as well. For example, the risks may be evaluated in light of specific concerns arising from the stage at which a product is in the development cycle, whether the employee is needed to finalize a project or transition the employee's work, or whether the employer will make an effort to retain the employee. Outside factors may also include the potential impact of the employee's departure on the company, the impact on the remaining employees, what message the departure sends (internally and externally), and what message the employer's response sends (to employees and others).

Applying Principle No. 1 to the offboarding and postemployment period, employers should use reasonable departure procedures, including exit interviews, that are calculated to obtain the return of company trade secret information and to understand the departing employees' commitment to protect trade secrets in their future employment, while respecting employees' interest in engaging in future employment and privacy interests.

Knowing what information departing employees had access to and where it presently resides can be critically important, whether for purposes of confidentiality and data security or for being able to identify and gather responsive electronically stored information in the context of pending or future litigation.

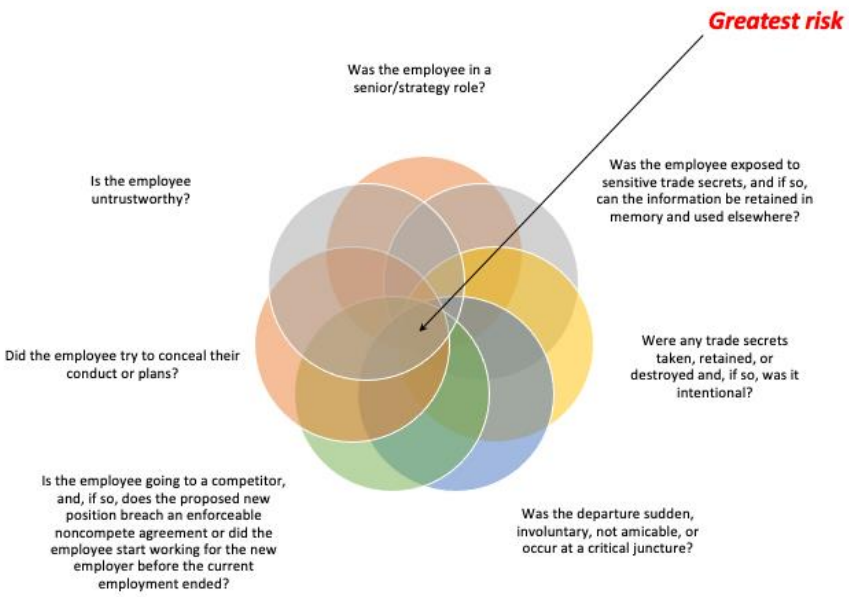
Some employee departures and exit interview processes are amicable, and some are not. This is not surprising as this is where the inherent tensions, as outlined in Principle No. 1, between an employer's interest in protecting its trade secrets and an employee's interest in engaging in future employment come to a head. The employer may be justifiably concerned that valuable trade secrets may be going to a competitor by way of this departing employee. The employee may be justifiably concerned that the employer may attempt to restrain the employee's ability to transition to another already accepted position or to seek future employment in his or her area of expertise, and that the employer may overreach with respect to its purported trade secret rights in order to do so. The goal is to facilitate an orderly transition respectful of both concerns, for the benefit of the former employer, the transitioning employee, and the new employer (if present).

A. ASSESSING THE LEVEL OF RISK

Key risk factors for potential trade secret misappropriation by departing employees can be summarized into the following seven broad questions:

- Was the employee in a senior/strategy role?
- Was the employee exposed to sensitive trade secrets, and if so, can the information be retained in memory and used elsewhere?
- Were any trade secrets taken, retained, or destroyed and if so, was it intentional?
- Was the departure sudden, involuntary, not amicable, or occur at a critical juncture?
- Is the employee going to a competitor, and if so, does the proposed new position breach an enforceable noncompete agreement, or did the employee start working for the new employer before the current employment ended?
- Did the employee try to conceal his or her conduct or plans?
- Is the employee untrustworthy?

In general, the more questions answered in the affirmative, the greater the risk—or at least the greater reason to investigate. Viewed as a Venn Diagram, the greatest risk is at the intersection of all seven circles:



Below is a discussion of these seven risk factors, together with additional, related questions.

- Was the employee in a senior/strategy role?

  All things being equal, the more senior an employee, the broader and deeper the employee's knowledge of company trade secrets will likely be—and therefore the greater the threat the employee is likely to pose.[43] However, this general rule is not always true. For example, while a senior executive may have broad-based knowledge of the company's trade secrets, the knowledge may be too shallow and generalized to pose an actual threat.[44]

- Was the employee exposed to sensitive trade secrets?

  "Access" to information is not necessarily the same as "exposure" to it. The mere fact that an employee had the ability to access trade secrets does not mean that the employee ever used that access. Accordingly, the potential threat comes from exposure to the secret.[45]

---

[43] Cases frequently distinguish between high-level employees and low-level employees as a proxy for their access to trade secrets and the threat they likely pose as a consequence. *See*, *e.g.*, Willis of New York, Inc. v. DeFelice, 299 A.D.2d 240, 242, 750 N.Y.S.2d 39, 42 (Supr. Ct. App. Div., 1st Dept. Nov. 19, 2002); Tactica Int'l, Inc. v. Atlantic Horizon Internal, Inc., 154 F. Supp. 2d 586, 608 (S.D.N.Y. 2001).

[44] *See*, *e.g.*, Int'l Bus. Machs. vs. Visentin, No. 11 Civ. 399(LAP), 2011 WL 672025 (S.D.N.Y. Feb. 16, 2011) (finding that defendant high-level executive's knowledge of plaintiff's trade secrets was too generalized to pose a substantial risk).

[45] *See*, *e.g.*, Harlan Labs., Inc. v. Campbell, 900 F. Supp. 2d 99, 108–09 (D. Mass. 2012) (noting that the employee not only had access to information but also accessed it).

- Assuming exposure, how sensitive/important are the secrets to which the employee was exposed?

  Not all information is created equal. Some information (for example, customer pricing information) may give a marginal competitive advantage, while other information (for example, product formulas like the secret formula to Coca-Cola) may be among the company's most valuable and therefore most competitively sensitive. While all of this information may be protectable as a trade secret, the consequences of the information falling into the hands of a competitor can vary greatly.

- Assuming exposure to sensitive trade secrets, can the information be retained in memory and used elsewhere?

  A former employee's (genuine) inability to recall information with enough specificity to use it poses much less of a risk than an employee who can retain and use such information.[46] For example, lengthy compilations of information may not be susceptible to memorization, whereas smaller amounts of information may be easily remembered in their entirety.[47] If the information can be memorized, it will be important to know how critical that information is. Further, of the information capable of being remembered, the critical inquiries are whether use or disclosure of that subset poses a threat,[48] and if so, for how long is it likely to be remembered, and how long does that relate to the shelf life of the information?

- Were any trade secrets taken, retained, or destroyed, and if so, was it intentional?

  The taking, retention, or destruction of information does not inherently pose a significant risk, though it can be a red flag. The inquiry must drill down to whether the employee was authorized to take, retain, or destroy the information, and if not, whether the conduct was intentional (in anticipation of the departure for purposes of later use) or inadvertent (for example, as part of routine backing up or an effort to take personal information). Further, if information was not taken physically or electronically, it is still possible that the employee memorized (or attempted to memorize) it, which should be investigated where that seems probable.[49] Consideration should be

---

[46] *See*, *e.g.*, Del Monte Fresh Produce Co. v. Dole Food Co., Inc., 148 F. Supp. 2d 1326, 1339 (S.D. Fla. 2001) (denying a preliminary injunction where, "[a]lthough [the former] had thorough knowledge of the business, the court finds credible [his] testimony that he cannot remember this information with precision.").

[47] *See*, *e.g.*, Free Country LTD v. Drennen, 235 F. Supp. 3d 559, 569–70 (S.D.N.Y. 2016) (the information was useful only in the aggregate and was too voluminous to have been remembered).

[48] *See*, *e.g.*, *id.* at 569–70 (the information was useful only in the aggregate).

[49] Oxford Global Res., Inc. v. Guerriero, No. Civ. A. 03-12078-DPW, 2003 WL 23112398, at *9 (D. Mass. Dec. 3, 2003) (injunctive relief would likely be warranted if defendants had taken steps to memorize confidential information); Fidelity Brokerage Servs. LLC v. Djelassi, No. 2015-2337-BLS1, slip op. at 6 & n.2 (Mass. Super. Ct.

given to whether the problem can be solved or mitigated if, for example, the employee returns the information.

Relatedly, an indication that the employee attempted to conceal his or her conduct may suggest consciousness of guilt.[50] Accordingly, employers will want to evaluate how the employee responded to the company's discovery that he or she had taken information.

- Was the departure sudden, involuntary, or not amicable, or did it occur at a critical juncture?

  Departures at critical junctures can increase the exposure a company faces from the exfiltration of trade secrets. Accordingly, the employer will need to evaluate the risk posed in light of the timing of the departure, especially where the departure comes at an inflection point for the company, affects the timing of a product launch or improvement, or otherwise affects the company's position in the marketplace.

  Similarly, departures that are involuntary or not amicable can increase the risk that the employee will be unwilling to protect the company's trade secrets or affirmatively motivated to harm the company, perhaps as a result of the view that because the company breached some real or perceived obligation to the employee, the employee owes nothing to the employer in return.

- Is there a need for a transition plan, or will the company attempt to retain the employee?

  Anytime an employee resigns, the employer may seek to retain the employee and thereby avoid the adverse impacts associated with the departure. However, where the employee does not remain and possesses unique knowledge that requires transfer to others, there may be a benefit to allowing the employee to stay long enough to facilitate such a transition or even temporarily engaging in a postemployment consulting relationship to facilitate the transfer. The benefits of facilitating a transition must be weighed against any continued access to trade secrets, which may be informed, in part, by whether the company and employee wish to maintain an ongoing, amicable postdeparture relationship.

- Is the employee going to a competitor, and if so, does the proposed new position breach any enforceable noncompete agreement, or did the employee start working for the new employer before the current employment ended?

Aug. 11, 2015) ("[T]he strategy of memorizing names and then calling [the former employer's] customers is suspect.").

50 Engility Corp. v. Daniels, No. 16-cv-2473-WJM-MEH, 2016 WL 7034976, at *9–*10 (D. Colo. Dec. 2, 2016) ("nearly every aspect of [defendant's] original story was either false or materially incomplete, forcing [defendants] into explanations that smack of one trying to escape a lie").

The risk of use or disclosure of a company's trade secrets its typically at its greatest when the employee's new employment is with a competitor. In such an instance, it becomes critical to understand the nature of the new role and whether and to what extent the company's trade secrets may be at risk of use or disclosure. In this regard, the focus of the risk posed by such individual's departure lies primarily on an assessment of the likelihood of use of the information in the employee's planned new employment.[51]

- Did the employee try to conceal his or her conduct or plans?

  Attempts to conceal conduct or plans may reflect that the employee is concerned that he or she has engaged in misconduct or is planning to violate his or her obligations to the company. Such efforts, however, do not necessarily reflect a malicious state of mind.

- Is the employee untrustworthy?

  Generally, an employee who has proven to be ethical and have a high degree of integrity is less likely to intentionally pose a threat to a former employer's trade secrets, although there may nonetheless be a risk of future disclosure, even though not intentional, in particular jobs.

- Has the employee been paid fully?[52]

B. MINIMIZING THE RISKS ASSOCIATED WITH EMPLOYEE DEPARTURES

Once the risk level has been identified, the employer and employee can (independently) evaluate the steps that each needs to take to minimize that risk. The steps set forth below are intended to be useful guidelines for situations with unusual risk and can be scaled back to meet the needs of lower-risk situations or where the employer or the employee lack the resources to implement all guidelines.[53]

The steps are presented in the order in which they typically arise in the ordinary course. However, the timing sometimes varies, and oftentimes some of the steps proceed in parallel.

---

51 For a detailed discussion of "threatened" misappropriation and claims of "inevitable" disclosure, please see *Sedona WG12 Trade Secret Equitable Remedies Commentary*, Section V.A. (Evaluating the Movant's Likelihood of Success on the Merits), pp. 25–37 & nn. 94-157, *supra* note 40.

52 Anytime an employer sues a former employee, it needs to expect counterclaims. A common counterclaim in that context is the failure of the employer to comply with their payment obligations, which can constitute both a breach of contract and a claim under applicable wage laws. Moonracer, Inc. v. Collard, Nos. 5:13–CV–455–BO, 5:13–CV–852–BO, 2015 WL 1275395, at *2 (E.D.N.C. March 18, 2015).

53 Note that the departure of an employee may have significant, tangential implications, including with respect to disclosures to shareholders of publicly traded companies, required or recommended notifications to clients and key relationships, even if simply for relationship management issues, and insurance coverage ramifications.

1. Rights and responsibilities of the employee

The employer should assess what reasonably constitutes its trade secrets and what reasonably belongs to the employee. The following should be reviewed and evaluated:

- *Applicable trade secret laws*.[54] Trade secret law imposes obligations on the employee for the protection of the employer's information that qualifies as a trade secret.

- *Agreements*.[55] Many types of agreements may speak to ownership of information created or developed during employment. Sometimes these are standalone agreements, while other times they are incorporated into an offer letter, employment agreement, or restrictive covenant agreement. Three of the most critical agreements tend to be: invention assignment agreements, nondisclosure agreements, and agreements imposing obligations on the employee to return company property (such as documents reflecting company confidential information).

  Regardless of where stated, the obligation to return documents and materials is an often overlooked obligation that can have significant consequences for an employee who fails to comply with it.

- *Company policies*. Like invention assignment agreements, company policies (as well as applicable law) often set the stage for the parties' expectations about what work is owned by the company and how it must be treated by employees.

There are exceptions to the prohibitions on an employee's use and disclose the employer's trade secret information, such as for purposes of whistleblowing under the Economic Espionage Act.[56]

2. Exit interviews

When an employment relationship terminates, exit interviews provide an opportunity for the soon-to-be former employer and the employee to understand and address the potential concerns relating to trade secrets. In particular, exit interviews allow the employer to understand where the employee

---

[54] Outside the scope of these guidelines are other areas of intellectual property law (patents, copyrights, and trademarks) and the common law of property.

[55] Sometimes external considerations impact an employee's access to these agreements. For example, the employee may not have retained a copy of these agreements and may not wish to ask for them in connection with a possible resignation, for fear of prematurely revealing his/her possible resignation. Addressing issues like these are beyond the scope of this *Commentary*.

[56] 18 U.S.C. §§ 1831-39 (as amended by the Defend Trade Secrets Act of 2016 (Pub. L. 114-153, 130 Stat. 376)). The Defend Trade Secret Act provides an express immunity from liability of an employee or consultant who disclose a trade secret in certain circumstances, specifically in confidence for the sole purpose of reporting or investigating a suspected violation of law or in a sealed filing in a lawsuit. However, the full parameters of this immunity (including, for example, who bears the burden of demonstrating applicability or inapplicability of the immunity and what conduct is immunized and what is not) are outside the scope of this *Commentary*.

is headed and assess the risks posed by that new role, and provide the employee an opportunity to assuage any concerns the employer may have and to understand and comply with the employee's various remaining obligations. The information garnered from such interviews will often result in the employer determining either that the departing employee does not pose a risk of trade secret misappropriation or that the departing employee does pose such a risk and steps therefore need to be taken to mitigate against them. Knowledge of this fact, accompanied with the employer's exit interviewer asking the departing employee to sign a certification with clear potential legal implications for doing so (and perhaps for not doing so), can understandably put the employee on the defensive. Skilled HR representation in conducting the exit interview can be critical in reducing these tensions and achieving a greater level of transparency in both directions that hopefully works to the benefit of both parties.

a. Importance of an exit interview

As a general matter, employers must be able to show that reasonable measures were taken to protect the secrecy of trade secrets in order to maintain the trade secret status of such information.[57] Employers can develop a false sense of security when employees sign confidentiality agreements during the course of their employment. While these agreements are helpful, they are not a panacea.[58] Employers must be able to show that reasonable measures were taken to (1) prevent the employee from taking their trade secret information to a competitor and (2) recover all copies of trade secret information from the departing employee, regardless of whether the information is in paper or electronic form.

Employers who fail to take reasonable actions—including to reclaim trade secrets that were in a departing employee's possession, custody, or control—can find themselves in the unenviable position of waiving trade secret status for that information before a court. Accordingly, proper exit interviews can not only serve their intended purpose of educating employees about their obligations and obtaining their compliance and assessing whether there is a problem, but can also help establish that the employer has taken reasonable measures to protect its trade secrets.

---

[57] *See*, *e.g.*, First W. Cap. Mgmt. Co. v. Malamed, No. 16–cv–1961–WJM–MJW, 2016 WL 8358549, at *8 (D. Colo. Sept. 30, 2016) *rev'd on other grounds*. First W. Capital Mgmt. Co. v. Malamed, 874 F.3d 1136 (10th Cir 2017) (requiring the company to establish irreparable harm in order to obtain injunctive relief); Uniform Trade Secrets Act, § 1(4)(ii) information purporting to be a trade secret must be "the subject of efforts that are reasonable under the circumstances to maintain its secrecy" of the information.

[58] Southern Field Maint. & Fabrication LLC v. Killough, No.: 2:18-cv-581-GMB, 2018 WL 4701782, at *6 (M.D. Ala. Oct. 1, 2018) ("Some states evaluate multiple factors in determining reasonableness, the presence or absence of a confidential disclosure agreement being just one factor, along with the nature and extent or precautions taken, the circumstances under which the information was disclosed, and the degree to which the information has been placed in the public domain or rendered readily ascertainable."); Boston Sci. Corp. v. Lee, No. 13–13156–DJC, 2014 WL 1946687, at *4 (D. Mass. May 14, 2014) ("It is not necessary that an impenetrable fortress be erected to retain legal protection for a trade secret. Instead, courts consider four relevant factors in determining whether plaintiffs asserting trade secret protections took reasonable security precautions: (1) the existence or absence of an express agreement restricting disclosure, (2) the nature and extent of security precautions taken by the possessor to prevent acquisition of the information by unauthorized third parties, (3) the circumstances under which the information was disclosed . . . to (any) employee to the extent that they give rise to a reasonable inference that further disclosure, without the consent of the possessor, is prohibited, and (4) the degree to which the information has been placed in the public domain or rendered 'readily ascertainable' by the third parties. Ordinarily, however, confidentiality agreements suffice to constitute reasonable protective measures." (citations omitted)).

While solid exit interview procedures are important, their usefulness depends on the skills of the interviewer(s). Depending on the risk posed by the departing employee, a company should consider have two members of management conduct the interview so that if there are any disputes as to what was said during the interview, there will be multiple witnesses. One of the managers should have an extensive understanding of the soon-to-be former employee's job duties. Including the employee's direct supervisor in the exit interview can be extremely helpful, both because the direct supervisor understands the employee's job duties and because the direct supervisor is often the person with the best understanding of the type of trade secret that the soon-to-be departing employee had access to and the customers or projects that the employee was working on. On the other hand, the departing employee may "clam up" if he or she is being interviewed by a manager, let alone two managers. Accordingly, depending on the circumstances, the employer may decide to use a less senior member of HR to conduct the interview. The HR staff member should be trained on how to conduct an effective exit interview (as should the managers if they are to conduct the interview). Further, if there are particular concerns (e.g., if the employee is going to a competitor), the employer should consider involving counsel to guide the interviewer about what to cover in the interview and how to address the existing concerns.

Striking the right tone is also critical, and should be tailored to the individual employee and circumstances and determined before the interview occurs. An exit interview does not happen in a vacuum. If the employee is leaving on bad terms—whether as a result of being fired, quitting due to perceived mistreatment, or arising from other circumstances—the employee may well be uncooperative during the exit interview independent of any intent to misappropriate any trade secrets, and this is best recognized and accounted for in advance to the extent possible. If an exit interview itself leaves an employee feeling that the company does not trust them, the interview itself may set up unwanted animus.

In some cases, the departing employee's responses during the exit interview may indicate that the employee has in fact engaged in improper behavior already.[59] In other cases, the interview may help confirm that nothing untoward has occurred or will occur and can leave the employer and the employee with positive feelings about the employment experience. To prevent escalation of any future concerns, the employer may want to give the employee a "point person" to contact with any questions or concerns in the future.

b. For the employer: Exit interview checklist

Prior to commencing an exit interview, the company should confirm that the departing employee signed the company handbook (if the company has one) and that the handbook included a policy that makes it clear to employees that the company reserves the right to inspect all company devices and company email, and that the employee should have no expectation of privacy in their use of company devices.

[59] In such instances, the exit interview may be a potential source of evidence to support a request for an injunction against the employee or their new employer. Such evidence may result from the employee repudiating their continuing obligations to the employer; the employee disputing that certain information is the employer's confidential information that they may not use it; the employee refusing to return company property; the employee lying during the interview; the employee being unable to explain how they can do the new job without misappropriating the current employer's trade secrets; or the employee revealing that they started working for a competitor while still employed by the current employer.

The following steps should be on an employer's exit interview checklist, which of course will need to be adapted to the particular departure and company culture:

- Inform the employee. The employee should be informed that in addition to any discussion of the reasons for the employee's departure, the exit interview is the opportunity for the employee to make a full and complete return of all paper and electronic company information in the employee's possession, custody, or control, including, but not limited to, all company computers and other storage devices that contain any company information, as well as company information stored on personal computers and other devices.

- Inform Human Resources, in-house counsel, and in-house information technology staff immediately if an employee refuses to participate in the exit interview. A departing employee's refusal to participate in an exit interview may reflect a threat of misappropriation. Accordingly, after such a refusal, steps should be immediately taken by the company to secure its information as discussed below.

- Retrieve company property. Employers should collect keys, access cards, uniforms, computers, tablets, smart phones, other assigned electronic devices (including USB storage devices), company credit or debit cards, and any other company property allocated to the employee. Retrieving company property will reduce the threat of misappropriation of trade secrets by eliminating the former employee's access to information. Such actions also may constitute evidence that the company has taken reasonable measures to ensure the continuing secrecy of the employer's trade secret information.

- Retrieve company records. Employers should ensure that all physical and electronic documents, records, data, plans, memoranda, reports, and other like materials are returned to the company. Employees should be asked where all of this information resides (either in paper or electronic form) so that the employee can assist the company, as part of the exit interview, to retrieve or forensically delete this information without the employee retaining copies.

- Remind the employee about continuing confidentiality obligations. An employee's duty to not misappropriate an employer's trade secrets endures even after the employment relationship has ended.[60] Employees may be unaware of this ongoing duty; in which case it is important that they be educated. They also may be under the misapprehension that while they cannot *disclose* the employer's trade secrets, they are permitted to *use* the employer's trade secrets, at least to the extent that they remember them. Having a record that the employer reminded the employee about their duty

[60] *See*, *e.g.*, Flexcon Co. v. McSherry, 123 F. Supp. 2d 42, 43 (D. Mass. 2000) (noting that the employee remains under a "duty not to disclose any confidential or trade secret information he learned during his employment").

to not misappropriate can assist in establishing reasonable efforts to ensure the secrecy of confidential information.

- Remind the employee about any restrictive covenants. Where an employee has signed nondisclosure, nonsolicitation, nonrecruiting, or noncompete agreements, the employer should remind the departing employee of the agreements' terms and the employee's obligations (if they are enforceable in the applicable jurisdiction). Reminding the employee will help increase the odds that the agreements are actually followed or raise any questions about their application and may be helpful evidence for the employer if the employee breaches them. The employee should also be given copies of these signed agreements so that the employee can reference their terms in the future.

- Obtain information on the employee's new employer. When an employee has resigned in favor of another job, the exit interviewers should try to gather information about the employee's new employer and the position and nature of the duties the employee intends to pursue. This could help the company assess the risks of misappropriation and unfair competition by the departing employee, but of course the employee may be understandably reticent to disclose this information for this very reason.

  The interviewer(s) should, however, also make clear to the departing employee that nothing said should be construed as an invitation to disclose the new employer's confidential information (if they employee happens to have any), and the employer does not want to receive any such information. The employer can, of course, also conduct its independent information search about the new position through public resources including any press releases announcing the new hire.

- Request the employee to sign a certification and acknowledgement. In most circumstances, either prior to or in conjunction with the exit interview, the interviewers should request that the employee search for and return all company property and information that was in the employees' possession, custody, or control, and then ask the employee to sign a certification that they have returned (and not retained) such property and information

  The company may also wish to include an acknowledgement to be signed by the employee that they have been reminded about and provided a copy of all applicable ongoing obligations to the employer. It is advisable to have the employee sign this same acknowledgment during onboarding and again during offboarding to mitigate against concerns by the employee that the employer is imposing any new obligations.

  A company cannot force a departing employee to sign, nor should final wages be withheld, if the departing employee refuses to sign. However, the departing employee's refusal to sign the certification/acknowledgement may

be a sign of a threat of misappropriation. The interviewers should inform human resources immediately if the departing employee does not sign the certification or acknowledgement. If training programs and policies along the way have coached the employee to understand that he or she may not retain and use company property, the exit interview and certification should be simply a continuation of those policies and practices—or provide an opportunity for the employee to raise specific questions.

- Request permission to inspect the departing employee's devices containing company information. Ideally, the employee has signed an agreement—or at a minimum, the company has a policy—by which the employee has granted permission to the company to inspect any personal devices onto which the employee has placed company information or through which the employee accessed company information or otherwise used for company business. Regardless, if personal devices were used for work or to access or store company information, the company should consider asking the departing employee's permission to inspect the employee's personal computer, smart phone, removable storage media (such as USB thumb drives), cloud backup and synchronization accounts, social media accounts, and other similar technology for company trade secrets or sensitive information. If the employee consents, the company can conduct an appropriate review, preservation, or deletion protocol, typically, in the employee's presence, with the employee's cooperation, and subject to a reasonably tailored, targeted protocol that respects the employee's privacy interests. If the employee does not consent, this is potentially a sign of a threat of misappropriation.

- Eliminate the departing employee's access to company networks. The company must ensure that the departing employee no longer has access to company networks. The exit interviewers must confirm with IT that all passwords, remote access codes, and virtual private network (VPN) numbers the departing employee once used to access the company's system are disabled.

- Ensure the departing employee is fully paid all wages due. Depending on the particular state's laws, employers may be required to pay the departing employee's final wages (including all accrued but unused vacation time) on the employee's last day of work.[61]

- Conclude the exit interview. The exit interview should then conclude. The departing employee will need to retrieve his or her personal items and leave the company's premises.

[61] This aspect of the exit interview, as well as that pertaining to health insurance, COBRA, and other benefits, is beyond the scope of these guidelines.

c. For the employee: Participating in exit interviews

Employees generally should participate in the exit interview process, and do so in good faith. Refusing to do so could create significant unwarranted suspicion, whereas cooperating with exit interviewers may reduce the likelihood of a misappropriation lawsuit.[62]

This does not mean that, absent contrary contractual obligations, departing employees have an obligation to provide any information that may be requested[63] or that they should necessarily volunteer information or be fulsome in the responses and information they provide. But absent important tactical or strategic reasons,[64] they should in most instances respond to reasonable and appropriate exit interview questions. An important reason for doing so is that when a departing employee refuses to reveal their postemployment plans, the employer may (perhaps incorrectly) infer a consciousness of guilt, i.e., that the refusal reflects the employee's belief that the new job violates some ongoing obligation to the former employer.

In all circumstances, even if the employee chooses not to answer particular questions, any questions that the employee does answer should be answered truthfully. Lies will raise concern by the former employer and could be used in litigation to suggest that the employee cannot be trusted.

As a general matter, allowing the company to investigate whether former employees have any trade secrets on any of their devices will help employees demonstrate that they intend to comply with their obligations and have no interest in retaining company information. To the extent that they have concerns about protecting their private information, they should raise those concerns with the interviewer. For example, where the employee has personal information on the employer's devices or on personal devices the company wishes to inspect, the employee should ask what steps can be taken to protect personal data from being accessed, disclosed, taken, or destroyed.

By cooperating in the exit interview, former employees may also reduce the chances of implicating their new employer in a potential misappropriation of trade secrets claim. Given that most employers ask their new hires to represent that they have not brought the trade secrets of their former employer to their new employer, being able to state that they fully cooperated in the exit interview may support such a representation.

Further, employees may wish to ask for permission to take information, or assistance in taking their own information.[65] If information has already been taken, it may be best for the employee to alert

---

62 Cooperation during the exit interview is a separate analysis from whether an employee should cooperate with ongoing business activities, such as transitioning their responsibilities to a new person or otherwise facilitating a smooth departure.

63 There may be contractual obligations that can alter an employee's duties. Any such obligations, including their enforceability and the consequences of a breach, should be evaluated before refusing to answer an employer's questions.

64 There may be many appropriate reasons for an employee to refuse to disclose information about their plans, including, for example, confidentiality obligations to their new employer. However, before refusing to answer the employer's questions, the employee should balance the reasons for refusing against the likely emotional impact on the current employer and the potential adverse inferences the employer may draw, and should consider consulting on this issue with the new employer or seeking legal advice from a lawyer.

65 Employees who have no intent to misappropriate information should avoid unnecessarily accessing, copying, or downloading company confidential information shortly before their employment terminates. If they believe they

the employer that he or she has information, and ask the employer how it would like that information handled. The timing of these conversations may be affected by the circumstances of the departure (an amicable resignation versus a "for cause" termination, for example).

Employees should sign a certification or acknowledgment that they have taken no information only if they are certain that they have returned all devices and trade secrets to their former employer. If they have not yet returned all such devices and information or have questions about issues concerning personal information (such as personal photos or financial records), employees should raise their questions and indicate that they need to complete the return of such devices and information before signing.

d. For the Employer: Information technology security

In many instances, immediately after the exit interview concludes, particularly in the case of high risk departures, the company will want to sequester and preserve departing employees' computers, company-issued cell phones, external hard drives, and other information technology, particularly where a departing employee had access to electronic versions of company trade secrets. A proper chain of custody for these devices and the information that was on them should be established, and, ideally, the devices should not be reissued to a new employee until the company is satisfied that it no longer needs them to investigate an employee's conduct or pursue a claim against the employee. Organizations that need to repurpose computer devices will want to consider whether preserving an electronic image of the device is economically feasible as failure to do so may result in the loss of important data and evidence.

If an investigation is warranted, any such investigation should be conducted on forensic copies of hard drives (or other storage media). Limiting the forensic investigation to the copies will maintain forensic integrity of a company's investigation by demonstrating that no original storage devices or hard drives had any new metadata placed on them that could create the appearance that the company was trying to make it look like the former employee engaged in wrongdoing. These copies will still show the same internal volume serial number as the original hard drives so that they can be authenticated for evidentiary purposes in court.

The company should be aware of its data retention and deletion policies and protocols, and assess whether to make an image of the former employee's email account.[66] A review of the employee's email activity can then be undertaken if there is reason to suspect misconduct.

Although the nature and context of the departure will inform the need for and appropriateness of these preservation, imaging, and forensic-review steps, ideally the devices and email should be preserved regardless of whether the company intends to engage in deeper examination of the

have a legitimate need to do so, they should generally confer with their supervisor or human resources so as to negate an inference that they were conducting themselves covertly because they knew they were engaged in wrongdoing.

66 The image should include the entire account (including, at a minimum, the inbox, outbox, sent items, and deleted items folders) but, if preserving the entire account is not feasible, the image should typically include the 60-90 days, or even up to six months, before the employment ended.

departing employee's activities. This is because the company may not know at that time whether the departing employee has been or will be engaging in unfair competitive activities.

Further, it is important that any forensic investigation not be undertaken without first consulting with legal counsel (in-house or outside) and using qualified forensic investigators who have expertise both in forensic protocols and, where necessary, testifying as to the acts of misappropriation engaged in by the former employee.

Once the forensic investigation has concluded, devices should not be wiped if the company discovered a concern during the forensic investigation. In that case, the device should be kept in a secure location and not reissued to another employee. However, if no problems were discovered, the company may follow its normal protocols, including wiping and initializing the devices and reissuing them to a new user.

C. DEPARTURE PROCEDURES

1. Reminder letters

After a former employee has completed the exit interview and left the company, the company should consider sending the former employee a reminder letter.[67] In contrast to "cease and desist" letters, which threaten enforcement of the employer's postemployment rights, reminder letters are routine communications, typically cordial in tone,[68] and are appropriate when the employee cooperated with the exit interview process and when the company does not have reason to suspect that the employee misappropriated company property or trade secrets.

Reminder letters are crafted to do what their name suggests: remind employees of their continuing responsibilities. In most instances, these letters should include copies of any confidentiality, noncompete, nonsolicitation, or any other relevant enforceable agreements signed during the course of employment—even if they were given to the employee during the exit interview. The more instances the company can show that they were trying to enforce its agreements and protect trade secrets, the stronger the company's position will likely be in any future lawsuit.

The reminder letter should inform the former employee that the law does not allow trade secrets gained while working for the company to be used or disclosed for any reason. Reminder letters can also address a former employee's social media accounts. An employer may wish to ask the former employee to update his or her social media accounts to reflect the fact that they no longer work at the company.

Reminder letters need not be sent to every departing employee. However, employees who had access to trade secrets should generally receive one. And, if the letter is sent when the employee is no longer employed, the letter should not include *the substance* of any trade secret information.

---

67 Typically, the reminder letter need not be a separate, standalone document; in many instances, it can be part of a routine exit letter or other communication to the departing employee.

68 In some instances, for example, when the employee participated in a key strategy meeting shortly before announcing their departure, the letter may take a more pointed tone, though not necessarily asserting misconduct or threatening legal action. In such instances, the letter should generally be a standalone communication, rather than part of another, routine communication.

2. Managing the impact of employee departures on remaining staff

The resignation or termination of a key employee or group of employees has the potential to trigger a variety of issues for the company. The departure can cause morale among the remaining employees to suffer. And the remaining employees may have trade secret information that they may intentionally or unintentionally disclose to the departed employee(s) whom they may remain in communication with. These same remaining employees may have information of the conduct of the departing employee(s) conduct that might be critical to help the company to protect its trade secrets.

Oftentimes, it makes sense for the company to get ahead of the issue and assess what concerns might be raised by the departure(s) and determine what reassurances can be provided to the remaining employees. For example, when a senior executive leaves, particularly at a critical juncture for the company, remaining employees may be concerned that the departure signifies uncertainty about the company's future. For a public company, similar perceptions may arise in the public eye.[69]

When a long-term or beloved employee leaves, remaining employees may consider their former colleague to still be in the "circle of trust" and be willing to continue to share trade secret or legal strategy information with him or her. Or the remaining employees may be loath to disclose misconduct by the departing employee of which they are aware. These issues may be exacerbated if the former employee is sued by the company, insofar as remaining employees may be upset that the employer is suing their former colleague and friend. Some remaining employees may also be called upon to testify against the former employee. Balancing what is said to remaining employees and getting their cooperation when needed can be a difficult task. As a general matter, the less said, the better—and the employer should avoid disparaging the former employee.[70]

Instead, the employer should explain, in general terms, the reasons for the employee's departure, provide assurances that the company will weather the change, and, where warranted, may inquire about any ongoing communication with the former employee and whether the remaining employees are aware of any misconduct either before or after the former employee left. It will typically be important to explain the significance of the issues in general and reinforce with the remaining population that the company takes the protection of its information very seriously. To the extent applicable, the company should also explain that it will be taking only those steps necessary to protect its interests—and those of the remaining employees. This discussion will help to assuage concerns, and have the added benefit of reminding employees of how to conduct themselves if and when they decide to leave the company.

In general, but particularly in circumstances where multiple people leave or where the company is concerned about the solicitation of its remaining employees, the company should recognize that anything said to the remaining employees may make its way back to the former employee. Discretion is therefore all the more important, as is reminding the remaining employees that they are

---

[69] If the company is publicly traded, there may be significant fallout when information of the departure—especially of key employees—becomes public. This is something that the company may wish to address as a public relations matter. However, what the company can and cannot say, and when and how it can provide this information, are outside the scope of this *Commentary*.

[70] One of the concerns that arises is that the former employee will assert that he has been defamed by the employer. While some states have qualified immunity for statements made to remaining employees, this issue is outside the scope of this *Commentary*.

not to share any confidential business information with the former employee.[71] The focus should always remain on company's reasonable efforts to protect its information (and any other protectable interests) and the remaining employees.

3. Notifying the new employer

In appropriate circumstances, a copy of the reminder letter (or even a separate letter) may be sent to the former employee's new employer. Sending such letters to the new employer can give rise to claims by the former employee that the former employer tortiously interfered with the relationship with the new employer or defamed the employee.[72] Accordingly, before doing so, the former employer should consider and evaluate the competing risks (for example, the risk that the employee will assert a claim, and the risk that the employee may not comply with, or even inform the new employer of, his or her ongoing obligations to the former employer). If a letter is sent to the new employer, the now former employer should not make false or unsupported accusations or to defame the employee.

D. REDUCING THE RISK OF MISAPPROPRIATION CLAIMS BY THE FORMER EMPLOYER

Departing employees and the companies they go to work for must always be careful to avoid misappropriating the former employer's trade secrets, not just intentionally, but inadvertently as well. While getting the "keys to the kingdom" of a competitor could be tempting, it will likely result in liability for misappropriation, expensive litigation that could drag on for years and other significant adverse consequences for all involved. Consequently, companies and their employees should be as careful to avoid engaging in or benefiting from misappropriation and should instead follow the guidance provided above from the beginning of the employment life cycle. In these and other respects, while the employment life cycle comes to an end for one employer-employee relationship, it is just the beginning of the next.

---

71 Employees should also be told how to respond to any inquiries they may receive concerning the former employee. For example, while employees may wish to protect the privacy of the former employee, industry regulations may require certain disclosures. *See*, *e.g.*, FINRA Regulatory Notice 19-10 (Customer Communications) (requiring customers, upon inquiry, to be provided certain information about a departed registered representative).

72 Oftentimes, agreements with the employee will contain a provision authorizing the former employer to notify the new employer.

The Sedona Conference Working Group Series & WGS Membership Program

"DIALOGUE DESIGNED TO MOVE THE LAW FORWARD IN A REASONED AND JUST WAY."

The Sedona Conference was founded in 1997 by Richard Braman in pursuit of his vision to move the law forward in a reasoned and just way. Richard's personal principles and beliefs became the guiding principles for The Sedona Conference: professionalism, civility, an open mind, respect for the beliefs of others, thoughtfulness, reflection, and a belief in a process based on civilized dialogue, not debate. Under Richard's guidance, The Sedona Conference has convened leading jurists, attorneys, academics, and experts, all of whom support the mission of the organization by their participation in conferences and the Sedona Conference Working Group Series (WGS). After a long and courageous battle with cancer, Richard passed away on June 9, 2014, but not before seeing The Sedona Conference grow into the leading nonpartisan, nonprofit research and educational institute dedicated to the advanced study of law and policy in the areas of complex litigation, antitrust law, and intellectual property rights.

The WGS was established to pursue in-depth study of tipping point issues in the areas of antitrust law, complex litigation, and intellectual property rights. It represents the evolution of The Sedona Conference from a forum for advanced dialogue to an open think tank confronting some of the most challenging issues faced by our legal system today.

A Sedona Working Group is created when a "tipping point" issue in the law is identified, and it has been determined that the bench and bar would benefit from neutral, nonpartisan principles, guidelines, best practices, or other commentaries. Working Group drafts are subjected to a peer review process involving members of the entire Working Group Series including—when possible—dialogue at one of our regular season conferences, resulting in authoritative, meaningful, and balanced final commentaries for publication and distribution.

The first Working Group was convened in October 2002 and was dedicated to the development of guidelines for electronic document retention and production. Its first publication, *The Sedona Principles: Best Practices Recommendations & Principles Addressing Electronic Document Production*, has been cited favorably in scores of court decisions, as well as by policy makers, professional associations, and legal academics. In the years since then, the publications of other Working Groups have had similar positive impact.

Any interested jurist, attorney, academic, consultant, or expert may join the Working Group Series. Members may participate in brainstorming groups, on drafting teams, and in Working Group dialogues. Membership also provides access to advance drafts of WGS output with the opportunity for early input. For further information and to join, visit the "Working Group Series" area of our website, https://thesedonaconference.org/wgs.

The Sedona Conference Working Group 12 on Trade Secrets—List of Steering Committee Members and Judicial Advisors

The Sedona Conference's Working Group 12 on Trade Secrets Steering Committee Members and Judicial Advisors are listed below. Organizational information is included solely for purposes of identification.

The opinions expressed in publications of The Sedona Conference's Working Groups, unless otherwise attributed, represent consensus views of the Working Groups' members. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any organizations to which they may belong, nor do they necessarily represent official positions of The Sedona Conference. Furthermore, the statements in each publication are solely those of the non-judicial members of the Working Group; they do not represent judicial endorsement of the opinions expressed or the practices recommended.

Steering Committee Members

James Pooley, James Pooley PLC—WG12 Chair
Victoria Cundiff, Paul Hastings—WG12 Vice-Chair
Monte Cooper, Goodwin Procter LLP—WG10-WG12 Steering Committee Liaison
David Almeling, O'Melveny
Russell Beck, Beck Reed Riden LLP
Nicole D. Galli, ND Galli Law LLC
Charles Tait Graves, Wilson Sonsini
Randall E. Kahnke, Faegre Drinker
Elizabeth McBride, Applied Materials, Inc.
Robert Milligan, Seyfarth Shaw
Patrick J. O'Toole, Jr., Weil, Gotshal & Manges LLP
Elizabeth Rowe, University of Florida, Levin College of Law

Judicial Advisors

Hon. Gail A. Andler (ret.), JAMS; Superior Court of California
Hon. Laurel Beeler, U.S. Magistrate Judge, Northern District of California
Hon. Hildy Bowbeer, U.S. Magistrate Judge, District of Minnesota
Hon. Denise Cote, U.S. District Judge, Southern District of New York
Hon. James L. Gale, North Carolina Business Court
Hon. Paul Grewal (ret.), Facebook, Inc.; U.S. Magistrate Judge, Northern District of California
Ron Hedges, former U.S. Magistrate Judge, District of New Jersey
Hon. Faith S. Hochberg (ret.), Hochberg ADR, LLC; U.S. District Judge, District of New

Jersey
Hon. James P. Kleinberg (ret.), JAMS; Superior Court of California
Hon. Laurie J. Miller, Fourth Judicial District, Minnesota
Hon. Donald F. Parsons (ret.), Morris, Nichols, Arsht & Tunnell LLP; Court of Chancery, Delaware
Hon. Joseph R. Slights III, Court of Chancery, Delaware
Hon. Gail J. Standish, U.S. Magistrate Judge, Central District of California
Hon. Bonnie M. Wheaton, Chancery Division, Illinois
Hon. Christine A. Ward, 5th Judicial District of Pennsylvania
Hon. Nina Y. Wang, U.S. Magistrate Judge, District of Colorado
Hon. Christopher P. Yates, 17th Circuit Court, Michigan