

Required Reading

2.1 - Sharing Trade Secrets with Other Organizations, Sedona Working Group 12 on Trade Secrets (August 2022)

Sharing Trade Secrets with Other Organizations
Sedona Working Group 12 on Trade Secrets
(August 2022)

Table of Contents

I.	Introduction	1
II.	Reasons For Sharing Trade Secrets With Other Organizations.....	3
A.	Due Diligence On A Potential Relationship	3
1.	License	4
2.	Supply Or Services Agreement With A Vendor Or Independent Contractor	4
3.	Joint Venture, Joint Development Or Other Collaboration	4
4.	Sale Of Goods Or Services	4
5.	Merger/Acquisition Or Sale Of All/Substantially All Assets.....	4
6.	Investment, Including Securitization For Debt Financing	4
7.	Regulatory Approval.....	4
B.	Conducting Business During A Relationship.....	4
1.	Licenser/Licensee.....	4
2.	Purchaser/Seller, Including A Vendor Or Independent Contractor	4
3.	Joint Venturers, Joint Developers Or Other Collaborators	4
4.	Seller/Customer	4
5.	Seller/Buyer In Connection With A Merger/Acquisition Or Sale Of All/Substantially All Assets	4
6.	Investee/Investor Or Debtor/Creditor	4
7.	Regulated/Regulator.....	4
III.	Trade Secret Sharing Tools Available Before, During And After Due Diligence Or A Relationship.....	5
IV.	Considerations Before Due Diligence Or A Relationship	6
A.	Personnel Involved.....	6
B.	Assets At Issue	7
1.	Identification Of Trade Secrets To Be Shared	7
2.	Identification Of What Is Not Part Of The Trade Secrets To Be Shared.....	9
3.	A Schedule For Potentially Sharing Additional Trade Secrets.....	9
C.	Protective Measures Before Sharing Trade Secrets.....	9
1.	Contractual Tools	9

2.	Physical Tools	16
3.	Technological Tools	19
V.	Considerations When Conducting Due Diligence Or In A Relationship	22
A.	Identify Assets At Issue	22
1.	Identification Of Trade Secrets Shared	23
2.	Identification Of Trade Secrets Or Other Assets Modified Or Jointly Developed.....	26
B.	Protective Measures When Sharing Trade Secrets	28
1.	Updating Contractual Tools, Including To Track And Control Sharing.....	28
2.	Updating Physical Tools, Including To Track And Control Sharing.....	28
3.	Updating Technological Tools, Including To Track And Control Sharing.....	29
VI.	Considerations When Ending Due Diligence Or A Relationship	30
A.	Potential Problems When Ending Due Diligence Or A Relationship	31
1.	Failure To Update And Finalize Identification Of Trade Secrets Shared, Modified or Jointly Developed.....	31
2.	Trade Secrets Not Returned/Destroyed When Due Diligence Or Relationship Ends	32
3.	Subsequent Work Relating To Trade Secrets Is Performed By The Receiving Party Or Receiving Party Personnel Who Subsequently Work Elsewhere And Perform Work Relating To Trade Secrets	33
4.	Receiving Party Hires Or Retains Disclosing Party's Present Or Former Personnel	34
5.	International Sharing Of Trade Secrets	35
B.	Potential Solutions When Ending Due Diligence Or A Relationship	37
1.	Perform Obligations in Contractual Tools.....	37
2.	Update Physical Tools	37
3.	Update Technological Tools	37
VII.	Appendices	38

I. Introduction

To be a trade secret, secrecy need not be absolute. In that regard, the law accommodates marketplace reality: realizing economic gain from a trade secret often requires the owner to disclose the trade secret to an outsider for evaluation, use or regulatory approval. A key aspect of such disclosure is that the trade secret be reasonably protected under the circumstances.

Despite the recognized need to exchange information in the real world, little written guidance has been provided to entities that must or want to share trade secrets with another organization. In particular, there is little written guidance on protecting trade secrets before, when, and after they are shared.

Such sharing might occur, for example, (1) between businesses exploring a potential relationship or engaging in an actual relationship, such as a license or joint venture or (2) between a business and a regulator, where the business is seeking approval or responding to a regulatory inquiry. Each scenario raises significant confidentiality concerns, which arise in connection with sharing the trade secrets, as well as subsequent disentanglement from or winding down or termination of any exploration or relationship. Such subsequent concerns are akin to concerns that arise in connection with employee departures¹.

Typically, a trade secret owner will share a trade secret with another organization only in exchange for an acceptable commercial benefit, such as economic gain or obtaining regulatory approval. That benefit comes with attendant risk, and balancing such benefit and risk is an important consideration when exploring, engaging in and, if or when necessary, disentangling from or winding down or terminating a relationship.

A key, but not unique, risk in business-to-business sharing is trade secret status can be lost if reasonable protective efforts to maintain secrecy are not made. What can be unique in this commercial context is how to address that risk. Overall, due to the tension between disclosure and protection, sharing should take place only after the disclosing party, e.g., the trade secret owner, secures suitable and verifiable protective efforts from the receiving party. Such efforts can be specified or embodied in contractual, physical and technological tools that define, document and control the receiving party's acquisition, access, disclosure, use, protection, return and destruction of the trade secrets.

This *Commentary* addresses the risk-benefit balance by focusing on protecting trade secrets before, during and after sharing, while not unreasonably hampering the receiving party's business operations. As noted above, such protection can be achieved through contractual, physical and technological tools. In more specific terms, those tools can include listing and identifying the trade secrets that are

¹ The Sedona Conference Commentary on Protecting Trade Secrets Throughout the Employment Life Cycle (March 2022) substantively analyzes, for example, trade secret considerations that arise in connection with employee departures.

shared, designating specific individuals with whom the trade secrets are or can be shared, specifying the purpose of the sharing and, as noted above, defining, documenting and controlling the receiving party's acquisition, access, disclosure, use, protection and, if or when necessary, return or destruction of the trade secrets and corresponding materials or embodiments. Importantly, any such tools and, more broadly, any trade secret sharing, whether for commercial or regulatory purposes, will create an evidentiary record that may be part of subsequent litigation or arbitration involving one or more of the shared trade secrets. Such a possibility can inform choices about which tools to employ and how to employ them.

The goal of the *Commentary* is two-fold: (1) to identify potential issues when sharing trade secrets and (2) to suggest pragmatic, potential solutions in light of marketplace realities. Notably, there is no one-size-fits-all approach for sharing trade secrets outside the owner's organization, whether sharing trade secrets as stand-alone assets or as assets that are part of a broader transaction. As such, the potential solutions, which are sometimes described herein as recommendations, are not intended to be and are not mandatory in any or every situation.

This *Commentary* does not address whether any protections, tools, solutions or combination thereof constitutes reasonable efforts to maintain the secrecy of a trade secret because such a conclusion depends on the circumstances at issue and is a question of fact to be determined by a judge, jury or other fact finder.² This *Commentary* also does not address any data privacy laws or how they might impact trade secret sharing within the United States or between the United States and a foreign country.

² References in this *Commentary* to a "trade secret" are not meant to imply that a court or other authority, such as the U.S. International Trade Commission or an arbitrator, has concluded that the information is, in fact, a trade secret. Instead, a reference to a "trade secret" is a reference to an alleged or asserted trade secret. For more details regarding identification of trade secrets issues, see The Sedona Conference, *Commentary on the Proper Identification of Asserted Trade Secrets in Misappropriation Cases*, 22 SEDONA CONF. J. 223, available at: https://thesedonaconference.org/publication/Commentary_on_Proper_Identification_of_Trade_Secrets_in_Misappropriation_Cases.

II. Reasons For Sharing Trade Secrets With Other Organizations

A. DUE DILIGENCE ON A POTENTIAL RELATIONSHIP

Each due diligence and each relationship that involves sharing trade secrets typically involves uniquely situated parties and unique challenges, which, in many cases, are tied to unique sources or levels of risk, and unique approaches and solutions. In other words, the parties typically are organized differently, and have different resources, methods of operations, cultures, especially if the parties are based or operate in different countries, existing policies and procedures and levels of expertise with trade secrets and contract management. As to sources and levels of risk, a joint venture or joint development work, for example, may require greater diligence and forethought before and during a relationship than investment into or funding of a start-up or a relatively common transaction between a customer and supplier. As to unique approaches and solutions, a confidentiality or non-disclosure agreement (NDA) is a common tool used to protect trade secrets, but the rights and obligations specified in an NDA can be impacted by multiple factors, including the parties' respective make-up (noted above) and the specific trade secrets at issue. These topics are more fully discussed below.

Commented [1]: Some comments have referenced degree of sensitivity, highly confidential vs. confidential information, and similar terminology. Some of those comments may be based on experience, e.g., how certain companies label/characterize certain information. Does any company label its trade secrets, as opposed to "confidential information," with different adjectives, such as "highly secret," "top secret," "really really secret" or (merely) "secret"? Or are all trade secrets labeled "trade secret," "secret" or with the same label/level of treatment? We should think and be careful about stratifying shared trade secrets into secret, highly secret, top secret, confidential, highly confidential, sensitive, highly sensitive, etc. buckets. Information is a trade secret or it is not; agreed? Value (which can vary and be fluid) is a different question and shows that a label (i.e., an incorrect label) can be as risky as it is helpful. So, these labels seemingly can be a practical, internal information management/protective measure tool that a disclosing party uses, e.g., to control internal access to its trade secrets. But that's different from creating a trade secret light or trade secret, jr. status in a sharing arrangement. Aren't parties creating a significant problem by (1) sharing and protecting "trade secrets" one way and (2) sharing and protecting "highly secret trade secrets" a 2nd way? If that's a commercially acceptable approach, then let's address it as such. As to that approach, it creates stratified/varied protective measure obligations for the receiving party and, in the process, introduces new risks of improperly/insufficiently protecting a "highly secret trade secret." And, if there's no stratification/variation in the receiving party's protection of trade secrets, then the different labels become that much more impractical if not useless (again, in the sharing context). If a disclosing company protects its trade secrets differently internally, then it seems that, for shared trade secrets, the highest level of its internal protections should be required of the receiving party. Another option, the lowest common denominator approach, seems, on its face, to be unreasonable.

1. License
2. Supply Or Services Agreement With A Vendor Or Independent Contractor
3. Joint Venture, Joint Development Or Other Collaboration
4. Sale Of Goods Or Services
5. Merger/Acquisition Or Sale of All/Substantially All Assets
6. Investment, Including Securitization For Debt Financing
7. Regulatory Approval

B. CONDUCTING BUSINESS DURING A RELATIONSHIP

1. Licensor/Licensee
2. Purchaser/Seller, Including A Vendor Or Independent Contractor
3. Joint Venturers, Joint Developers Or Other Collaborators
4. Seller/Customer
5. Seller/Buyer In Connection With A Merger/Acquisition Or Sale Of All/Substantially All Assets
6. Investee/Investor Or Debtor/Creditor
7. Regulated/Regulator

FDA (Pharma-Generics/Biomedical/Biologics-Biosimilars), Insurance, EPA, FOIA, Fracking, Agriculture, API (Application Programming Interface)

III. Trade Secret Sharing Tools Available Before, During And After Due Diligence Or A Relationship

Parties who share trade secrets often proceed through a sequence of (1) pre-sharing, (2) sharing and (3) post-sharing. In other words, the sequence has three general periods: (1) the pre-due diligence or pre-relationship period, (2) the due diligence or relationship period (3) the post-due diligence or post- relationship period. Of course, due diligence may or may not result in a relationship and there may be a wind down or disentanglement before the post-due diligence or post- relationship period.

There are three major categories of protective measures that a disclosing party may use to protect its trade secrets before, during and after the trade secrets are shared: (1) contractual tools; (2) physical tools; and (3) technological tools. Each category is discussed below.

[Proposed] Principle No. 1: Before and when trade secrets are shared, physical tools, contractual tools and technological tools should be used to protect, including to limit access to, the trade secrets, and those tools may be modified throughout the lifecycle of the relationship.

IV. Considerations Before Due Diligence Or A Relationship

A. PERSONNEL INVOLVED

For a disclosing party, a starting point for sharing trade secrets with another organization can be identifying and organizing individuals who will coordinate and otherwise be involved in the sharing (the Team). The Team members may be employees, agents or other representatives of the disclosing party. They will focus on the substance of, execution of and compliance with measures to protect the trade secrets and monitoring the receiving party's activities and compliance with its obligations.

Each Team member can be responsible for a specific area. Those areas can include project management (*i.e.*, communication and coordination with the receiving party and compliance with sharing procedures, including protective measures), subject matter expertise (*i.e.*, knowledge of the trade secrets), legal, security (*i.e.*, physical or facility security), information technology (*i.e.*, coordination of secure, electronic storage of and access to the trade secrets) and human resources (*i.e.*, knowledge of company policies and procedures relating to trade secrets). Each due diligence or relationship involving trade secret sharing is different, so a Team may include one or more of the foregoing or other individuals. For a small company, a Team may consist of only one or a few individuals. The volume and nature of the trade secrets, as well as the resources of a company, can also affect a Team's make-up.

A receiving party can have the same starting point, with a few modifications to the areas addressed by the Team. A receiving party Team also will focus on complying with its obligations and, in turn, avoiding missteps and disputes relating to shared trade secrets. As to those modifications, the receiving party Team member with subject matter expertise presumably possesses general subject matter knowledge, as opposed to knowledge of the trade secrets.

Notably, a disclosing party may request or require that a receiving party Team not include any individual who works with or on any competing technology or subject matter. A receiving party may agree to such a request or requirement or seek a narrower exclusion, such as any individual who researches or develops any competing technology or subject matter. Such an exclusion can benefit both the disclosing party and receiving party by reducing the risk of trade secret misappropriation or a breach of contract and a resulting dispute. Where such an exclusion is not feasible, and the disclosing party is still willing to share its trade secrets, gradually sharing the trade secrets in sequenced fashion or segmented fashion, *i.e.*, a part or parts of a trade secret are shared and then the rest of the trade secret is shared if the parties wish to proceed with the due diligence or relationship, may be viable options.

If the disclosing party and receiving party are actual or potential competitors, then a data room, which may be or include a clean room, is an option to consider. Data rooms are further discussed below.

Team members should be contractually bound to protect any trade secrets disclosed or received. At least for the disclosing party Team, such contracts may, and should, have existed prior

Commented [2]: It may make sense to include a Principle here, similar to the one before identifying the assets at issue:

Principle No. IV-X – Before parties are engaged in due diligence or a relationship that will involve sharing trade secrets, the parties should agree in writing on point person business and, if necessary, legal, contacts who will be on either end of the communications regarding a potential business venture. Keeping the circle small, at least initially, balanced with controlled prospective sharing of trade secrets protects both sides of the exchange.

to any sharing. The use of such contracts, or supplementation of existing contracts, in connection with the sharing is further discussed below.

Finally, some employers periodically train, or at least remind, employees about the value of and obligations to protect trade secrets. Similarly, the disclosing party and receiving party can train or remind Team members and others involved in the trade secret sharing about their obligations relating to trade secrets in general and the trade secrets to be shared. The frequency and extent of such training or reminding can be affected by the duration of the due diligence or relationship.

B. ASSETS AT ISSUE

Principle No. IV-1 – Before parties are engaged in due diligence or a relationship that will involve sharing trade secrets, the parties should agree in writing on the types of trade secrets, by category, intended to be shared, with the categories specific enough to make clear the types of information the receiving party is obligated to protect throughout the due diligence or relationship.

1. IDENTIFICATION OF TRADE SECRETS TO BE SHARED

Before due diligence or a relationship commences, the disclosing should determine, perhaps in collaboration with the receiving party, the categories, or types, of information that the disclosing party will share and that the receiving party will need to evaluate or effectuate the potential or actual relationship.

A disclosing party will be balancing two concerns when providing categories of information to the receiving party. On the one hand, the more detailed the categories, the greater the potential for jeopardizing information's trade secret status. On the other hand, categories that are too general may not provide the receiving party with an ability to understand or further understand the expectations for protective measures, the actual or potential relationship and the information in its possession that may be relevant and that it may need to or be obligated to share.

In some cases, both the disclosing party and receiving party will know, at the outset of their interactions and in light of the contemplated relationship, the categories of information to be shared. In other cases, there may be a greater need for collaboration between the parties. Ultimately, the disclosing party should describe the categories of information to be shared with enough specificity to make clear the types of information the receiving party will be obligated to protect throughout the due diligence or relationship. However, the categories of trade secrets should not identify, i.e., should not disclose, any trade secrets.

A subsequent step for the disclosing party is to gather the information in those categories that will be shared. Within those categories, some of the information may be trade secrets, some of the information may be information classified as confidential, sensitive, or proprietary, but that does not rise to the level, i.e., legal definition, of a trade secret, and some of the information may be publicly or generally known information.³ A disclosing party's appreciation for, and proper accounting of, those

³ A separate Commentary, [REDACTED], analyzes the existence of confidential information apart from trade secrets.

different types of information can become important where trade secrets and other information are submitted to a regulatory authority and submitted information is later sought through, for example, a Freedom of Information Act request. Additionally, if information is publicly or generally known, then a disclosing party can share that information without protection and, as a result, potentially save time, money and effort.

Once collected, a disclosing party should separate its trade secrets from the non-trade secret information so that the trade secrets can be readily tracked and, at the appropriate time, properly shared.

At this point, the disclosing party (1) should know the categories of trade secrets that may be shared and (2) should be able to identify, and should internally identify, the trade secrets that may be shared.

A trade secret that is identified is set forth with sufficient particularity.⁴ A prior Commentary addresses proper trade secret identification in litigation and the principles and guidance in that Commentary can be readily applied to trade secret identification in connection with due diligence or a relationship.⁵

Next, the disclosing party should account for any of its policies and procedures for identifying and protecting trade secrets, any applicable written agreements, such as NDAs, that protect trade secrets, any other contractual, physical or technological protective measures, or tools, such as marking, secure storage, segregation, limitation on access and monitoring of any of the foregoing.⁶ See *Scentational Technologies, LLC v. Pepsico, Inc.*, 13-cv-8645 (KBF), 2018 WL 2465370 (S.D.N.Y. May 23, 2018), *aff'd* 777 Fed. Appx 607 (Fed. Cir. 2019) (trade secret claim fails without contemporaneous records describing the trade secret, which was necessary to corroborate claim of joint invention).

⁴ A properly identified trade secret, i.e., a trade secret identified with sufficient particularity, is distinct from the categories of information, or general subject matter, eligible for trade secret status. See, e.g., 18 U.S.C. § 1839(3) (Defend Trade Secrets Act defining a “trade secret” as “all forms and types of financial, business, scientific, technical, economic, or engineering information,” regardless of the medium of storage, compilation or memorialization if “(A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information[.]”); and UTSA, §1(4) (“‘Trade secret’ means information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.”). The UTSA or a version thereof has been adopted in 49 States (the only exception being New York) and the District of Columbia.

⁵ See The Sedona Conference, *Commentary on the Proper Identification of Asserted Trade Secrets in Misappropriation Cases*, 22 SEDONA CONF. J. 223.

⁶ Examples of other contractual tools may include non-competition agreements and non-solicitation agreements.

Commented [3]: We can consider what, if anything, happens if the disclosing party does not designate shared information as a trade secret (TS). Seems like a good opportunity to draft an example of a provision (in the appendix) that addresses an inadvertent failure to designate information as a trade secret. Absent such a provision, suppose the disclosing party later wants to sue for “misappropriation” of confidential information (CI)? Can the CI now be a TS? Was TS status waived? If the disclosing party sues for breach of contract re the CI, ok. The possibility of a breach of contract action based on, e.g., misuse of CI seemingly increases the need to focus on CI-related contractual remedies, obligations, etc. (topics that can be mentioned, but are beyond our current charter). As for the provision, there may be a protocol to mark the info as a TS within x days of realizing it was not properly marked as a TS. With all of that, the reality is that TS and CI probably are going to both exist, at least acc. to some. But, for this Commentary and the principles, a focus on TS -- without ignoring CI -- is the more workable approach.

Commented [4R3]: Great idea about inadvertent disclosure and potential “claw back”

Commented [5]: Joint invention being a patent term, let's further analyze case -- and, as needed, clarify or edit parenthetical -- and supplement with additional case citation(s).

Commented [6R5]: Collaboration?

Where a disclosing party knows how it protects its trade secrets, it will be able to require corresponding protective measures from a party that receives its trade secrets during due diligence or a relationship. Ultimately, a proper protocol for sharing trade secrets with a third party needs protective measures that satisfy the legal standard of reasonable protective measures.⁷

2. IDENTIFICATION OF WHAT IS NOT PART OF THE TRADE SECRETS TO BE SHARED

3. A SCHEDULE FOR POTENTIALLY SHARING ADDITIONAL TRADE SECRETS

C. PROTECTIVE MEASURES BEFORE SHARING TRADE SECRETS

Sharing trade secrets with third parties increases the risk of (1) misappropriation, i.e., unauthorized acquisition, disclosure or use of the trade secrets, and (2) loss of secrecy and, as such, loss of trade secret status. An effective way to mitigate those risks is to take protective measures *before* any trade secrets are shared and be ready to timely enhance protective measures if and when sharing actually occurs.

As noted above, the three major categories of protective measures that a disclosing party may use to protect its trade secrets before, during and after the trade secrets are shared are: (1) contractual tools; (2) physical tools; and (3) technological tools. Notably, there is no one-size-fits-all approach to protective measures. Rather, protective measures must be reasonable under the circumstances to establish and maintain trade secret status. In practice, protective measures may be reasonable under the circumstances where they fall into one or more of those categories. Similarly, establishing reasonable protective measures under the circumstances does not require implementing all the specific examples of protective measures discussed below.

Principle No. __ - Where a party intends to share trade secrets with another party during due diligence or a relationship, it should take initial reasonable protective measures before any trade secrets are shared, with one of those measures being an appropriate confidentiality or non-disclosure agreement.

1. CONTRACTUAL TOOLS

A contract is often the starting point for protecting trade secrets before sharing them. More specifically, parties contemplating trade secret sharing often enter into a confidentiality or non-disclosure agreement (NDA) that governs the acquisition, access, disclosure and use of the trade secrets and imposes additional protective measures, such as secure storage, for the trade secrets.⁸

⁷ One of the requirements for trade secret status is that the information be the subject of reasonable protective measures. *See* 18 U.S.C. § 1839(3) (Defend Trade Secrets Act (DTSA)) *and* Uniform Trade Secrets Act (UTSA), § 1(4).

⁸ An executed NDA often is the culmination of a drafting and negotiating process. The process typically commences when the disclosing party sends an NDA to the receiving party, with the hope that the receiving party simply will sign and return the NDA. That may happen where the disclosing party possesses greater bargaining power, including greater resources. A more typical scenario, however, especially between two

An NDA typically serves several important purposes. First, an NDA provides notice to the receiving party of the categories of information, or general subject matter of, the disclosing party's trade secrets. Second, an NDA imposes on the receiving party contractual obligations to maintain the secrecy, or confidentiality, of the trade secrets and to refrain from accessing, using or disclosing the trade secrets in a manner not authorized by, or that exceeds the authorization provided in, the contract. Third, an NDA provides remedies to the disclosing party if the receiving party breaches any contractual obligations. Fourth, an NDA is, at once, an important protective measure and tangible evidence of reasonable protective measures, which must be taken for information to achieve trade secret status.⁹ In fact, an NDA is so important, or fundamental, as a protective measure, that the absence of an NDA likely will make proving the existence of a trade secret, *i.e.*, that reasonable measures were taken to protect the information at issue, more challenging and, as such, may eliminate a claim and remedies for trade secret misappropriation.¹⁰

An NDA is also like any other contract insofar as it may not address every issue or nuance that arises. For this reason, clear communication between the parties when negotiating an NDA is unsurprisingly important. If documented, communications between the parties may facilitate resolution of a subsequent error, confusion or dispute relating to the NDA and, depending on the existence and enforceability of an integration clause, may be evidence for use in litigation or an alternative dispute resolution process.¹¹

Commented [7]: Our focus here is trade secrets (TS). "Confidential information" (CI) is an issue that will arise and often is addressed in an NDA. The treatment of CI is something that is being addressed by another Commentary/group. So, if necessary, we can mention CI, but should be mindful of our TS focus and the other Commentary/group's CI work. An up-front comment or footnote that CI is being addressed by another Commentary and will not be substantively addressed in this Commentary makes sense.

Commented [8]: Great opportunity for the higher level purposes and the more specific provisions set forth below to be, or be the basis for, provisions in the appendix.

entities, is an NDA is executed after an exchange of revised drafts and negotiations. We raise this dynamic to illustrate there is no universally used NDA and, overall, each due diligence and relationship is unique. As such, this Commentary is not meant to provide and does not provide a one-size-fits-all suggestion, recommendation, or requirement for an NDA or anything else.

⁹ See note 7, *supra*.

¹⁰ See, e.g., *Abrasive 90 Inc. v. Weldcote Metals, Inc.*, 364 F. Supp. 3d 888, 898 (N.D. Ill. 2019) ("Failure to enter into nondisclosure or confidentiality agreements often dooms trade secret claims."). While not necessarily cast as such, an NDA is one of three common-sense, easily achievable protective measures that judges and juries readily understand and often expect to see. The other two common-sense, easily achievable protective measures are marking as "trade secret," "secret" or "confidential" a document or file that is or includes a trade secret, thereby providing notice of the information's status to those who access it, and limiting trade secret access to those persons with a "need to know" the trade secret.

¹¹ An integration clause is sometimes called a merger clause or entire agreement clause.

Definition of “Trade Secret”¹²

Sometimes, the term “trade secret” is not defined in an NDA.¹³ Rather, the term simply is included with the definition of “confidential information.” That approach may be convenient, but it often does not sufficiently focus the parties’ attention on the categories, or subject matter, of the trade secrets to be shared. Thus, parties who are about to share trade secrets should consider defining the term “trade secret” in an NDA, and that is true even if they decide to define and account for “confidential information” and include the term “trade secret” within the definition of “confidential information.”

Parties may have opposing views on how to define “trade secret” in an NDA. For example, the disclosing party may want a broad definition of the categories or subject matter to be shared, given that it wants to protect by contract as much of the shared information as possible. Conversely, the receiving party may want a narrow definition so that, for example, it is not broadly obligated or impaired or even foreclosed from present or future activity in a certain field. Other times, both parties may want to narrowly define “trade secrets” so that the sharing is focused and notice regarding the respective rights and obligations is correspondingly clear. In other words, a focused definition should facilitate the disclosing party’s efforts to collect and organize the trade secrets to be shared and result in the disclosure, receipt and management of fewer trade secrets. Where fewer trade secrets are at issue, the parties may save time, money and effort during the sharing and the overall risk or degree of harm and potential for a dispute can be reduced.

Notably, an NDA, like most contracts, provides a mechanism for the parties to amend a term or provision, such as the definition of “trade secret,” bearing in mind that, no matter what the definition of “trade secret” is, or is amended to be, no trade secret should be disclosed by that definition or within the NDA itself. The definition of “trade secret” also can include a procedural component. That is, a disclosing party typically is and should be obligated to mark a shared trade secret in a particular way so that the disclosing party knows what trade secrets are disclosed and the receiving party knows what trade secrets it receives just by looking at the document or file.

Additionally, an NDA can exclude information from the definition of “trade secret.” For example, “trade secret” would not include information that is or becomes generally or publicly known through no fault of the receiving party.¹⁴ However, if a trade secret becomes generally or publicly

¹² Historically, NDAs often have defined the information being shared as “Confidential Information,” with “trade secrets” included within that definition. However, the focus of this Commentary is trade secret sharing. As such, this Commentary addresses here a definition for “Trade Secrets.” Another Commentary will address the separate existence and status of confidential information and the relationship between confidential information and trade secrets. Thus, even if an NDA includes a definition of “Confidential Information” and even if that definition includes the term “trade secrets,” this Commentary addresses how an NDA can separately define “Trade Secrets.”

¹³ The definition of “trade secret” addressed here is a subject matter definition where the categories, or general subject matter, of the trade secrets are described. The legal definition of “trade secret” is not being re-defined or otherwise modified. As discussed herein, the legal definition is being applied. The applicable legal definition, whether under the DTSA, a State’s version of the UTSA or otherwise, can be accounted for in a choice of law provision within the NDA or would be determined during subsequent trade secret litigation.

¹⁴ See, e.g., 18 U.S.C. § 1839(3)(B).

known, how that situation unfolded and who is at fault may not be clear. One way for the disclosing party to potentially improve its ability to obtain relief under such circumstances is a provision where, on top of specific protective measures obligations, the receiving party is obligated to protect the shared trade secrets with measures of protection that meet or exceed the measures its uses to protect its own trade secrets or, if it has no trade secrets, then its most important confidential information.

An NDA also can exclude from the definition of “trade secret” information that is independently developed by the receiving party, i.e., developed without the use of the disclosing party’s trade secrets, or previously known by the receiving party, i.e., known prior to the date the trade secrets were shared. Such an exclusion may also be supplemented by a corresponding provision specifying how, and possibly a date by which, a receiving party can or must claim that it previously knew certain information.

The above discussion about the definition of “trade secret” illustrates the need to carefully draft and review an NDA and tailor it to the specific circumstances at issue. This is not to say that certain terms or provisions, such as a provision for amending an NDA, may not be relatively standard or common. But accepting boilerplate terms or provisions, which may be presented as take it or leave it, can be costly.

Moreover, a failure to include any exceptions whatsoever to the definition of confidentiality may erode its enforceability in a court of law.

The Parties to the NDA

Another issue that often arises when negotiating an NDA is who – which entities and which individuals -- will be parties to or otherwise bound by its terms. Where, for example, a transaction involves only two parties, i.e., one disclosing party and one receiving party, organized and operating in uncomplicated fashion, e.g., both are single-location companies with no affiliates, resolution of this issue can be relatively straightforward. However, where, for example, a transaction involves multiple parties organized and operating in complicated fashion, resolution of this issue can require greater inquiry and attention to detail and more specific NDA provisions. The parties should address, early in negotiations, their respective organizations and operations, including locations and affiliates, and which persons (e.g., affiliates, employees and other entities and individuals) will be parties to the NDA or otherwise be bound by its terms. A person may otherwise be bound by, for example, a written, executed addendum to the NDA, a copy of which can be timely provided to the disclosing party. Where multiple locations are in play because, for example, the disclosing party and receiving party are located in different jurisdictions, the parties can address basic but important issues, such as forum and venue selection and choice of law in the event a subsequent dispute arises.¹⁵ Where multiple locations are in play because, for example, an authorized affiliate or employee of the receiving party is in location X and another authorized affiliate or employee of the receiving party is in location Y, then the disclosing party should consider whether either location or jurisdiction poses challenges that can be resolved or should be avoided. Those challenges may relate to enforcement of the NDA, or a certain provision therein, in the event a subsequent dispute arises.

Commented [9]: Let's further develop this dynamic with respect to, e.g., private equity or similar entities. Digging deeper, the take it or leave it NDAs often include provisions that limit confidentiality obligations to a certain period of time. A big issue to address.

Commented [10]: Do we have a case cite or other authority for this proposition? Has a court ruled that you lose your trade secrets because your confidential information or trade secret definition was too broad?

¹⁵ These important issues are further discussed below.

The Purpose for Sharing Trade Secrets.

A key provision in an NDA is a provision that specifies the purpose for sharing trade secrets. Parties to an NDA often include and should include a provision stating the purpose for sharing trade secrets and the specific period during which the sharing can take place. A typical purpose is to evaluate a potential, future relationship between the parties, such as a license, sale of assets, merger or acquisition. In other words, any acquisition, access, disclosure and use of shared trade secrets is limited to that purpose. Any acquisition, access, disclosure and use of a shared trade secret for another purpose, such as advancing the receiving party's own commercial interests, is prohibited.

Specifying Physical and Technological Tools

An NDA, i.e., a contractual tool, should not be the exclusive means to protect shared trade secrets. Physical and technological tools, which are addressed in detail below, also should be used. NDA provisions can specify the physical and technological tools that will be used to protect shared trade secrets and, ultimately, these tools complement, embody and implement NDA provisions relating to protection, acquisition, access, disclosure and use of shared trade secrets.

How Trade Secrets Can Be Accessed, Disclosed and Used.

An NDA also may set forth the how the receiving party can access, disclose and use shared trade secrets. A provision addressing this issue may set forth the points of access for authorized individuals to acquire, review, disclose or use trade secrets and may also describe or identify specific individuals authorized to access, acquire, review, disclose or use trade secrets. An NDA also may specify that individuals authorized to access, acquire, review, disclose or use trade secrets must verifiably acknowledge -- e.g., in writing or by click -- applicable obligations each time such act occurs.

An NDA also can include a provision with prohibitions or limitations on when, where, why, how and by whom shared trade secrets may be acquired, accessed, disclosed and used.¹⁶ Importantly, only an individual with a need to know a trade secret should be authorized to acquire, access, disclose or use the trade secret. To that end, individuals, by name, title or category, with need-to-know status and such authority can be specified in an NDA, as can individuals, by name, title or category, who lack such status and such authority.

Temporal or Durational Limitation on Confidentiality Obligations

An NDA may include a temporal restriction or durational limitation on confidentiality obligations, it may provide that those obligations continue so long as at least one shared trade secret remains secret, it may provide that those obligations continue with respect to each trade secret for so long as the trade secret remains secret, or it may provide that those obligations continue in perpetuity. Parties should be aware that some courts may view an NDA as a contract that can negatively impact competition and, as such, may look skeptically at confidentiality obligation without a durational

Commented [11]: A prior draft included the following concept: "the circumstances, if any, permitting disclosure to individuals other than the 'need-to-know' individuals and who those other individuals are, by name, title or category." Include or not? Is there an example where this provision would be applicable? Is a general amendment clause (e.g., NDA can be modified by a signed writing) enough?

¹⁶ As explained above, an NDA can include a provision stating the purpose for sharing trade secrets. The "why" here entails a provision that, for example, prohibits or further limits a specific individual's or specific individuals' acquisition, access, use and disclosure of trade secrets based on the reasons for doing so.

limitation.¹⁷ Having said that, some trade secrets can exist forever, *i.e.*, they can exist until they are no longer secret, other trade secrets may have a shelf life because once executed they become public (in the case of a marketing strategy, for example) and other trade secrets may, after a period of time, become stale and have no value (in the case of cost or pricing data, for example). A key point here is that any durational limitation must be carefully assessed by both parties, and especially the disclosing party, as it can have a significant impact on trade secret status and the parties' respective rights and obligations.

Return or Destruction of Trade Secrets

An NDA can include a provision describing how the termination of the parties' due diligence or relationship affects the NDA. The provision may state that confidentiality and other obligations continue, despite termination, and that the receiving party must take certain steps to protect shared trade secrets, including, for example, returning or destroying the trade secrets in its possession. Importantly, an NDA can include a provision requiring the receiving party to acknowledge, in a signed writing, the specific trade secrets returned or destroyed and that no copy of any trade secret has been retained. As a practical matter, a return or destruction obligation is obligation of which the disclosing party should affirmatively remind the receiving party once the due diligence or relationship is terminated. Also, an NDA may set forth exclusions to the return or destruction obligation, such as: (1) documents or information that must be retained by the receiving party in order to comply with an applicable legal obligation, with such return or destruction promptly occurring upon termination of the legal obligation, (2) document or information back-ups in the ordinary course that are not accessible by any unauthorized person, where such back-ups will be destroyed, or permanently deleted, in the normal course of the receiving party's document retention or destruction policy, a copy of which the receiving party has provided to the disclosing party, and (3) where a dispute between the parties exists, documents or information relating to, or that reasonably may relate to, the dispute retained by the receiving party's outside counsel until the dispute is fully and finally resolved.

Remedies

An NDA can specify remedies for a breach of the NDA. Relatedly, an NDA can include three provisions that impact the availability of those remedies: (1) a pre-litigation dispute process; (2) choice of law; and (3) choice of forum and venue.

Pursuant to a pre-litigation dispute provision, the parties may be required to address, and attempt to resolve, any dispute, disagreement or claimed breach prior to commencing litigation. While each situation is unique, a disclosing party may be hesitant to agree to a time-consuming or involved

Commented [12]: Regarding the Carlson case in the footnote, let's address what was at issue, *i.e.*, trade secrets, confidential information, or both? We need to clarify that case and those issues, as well as the law (IL?) at issue.

Commented [13]: Do we want to further address deletion particulars or protocols?

¹⁷ See, e.g., *Carlson Grp., Inc. v. Davenport*, No. 16-CV-10520, 2016 WL 7212522, at *5 (N.D. Ill. Dec. 13, 2016) (invalidating a nondisclosure clause as unreasonable and noting that the omission of a temporal limitation bears on its reasonableness.) But see, e.g., 765 ILCS 1065/8 (b) ("This Act does not affect: (1) contractual remedies, whether or not based upon misappropriation of a trade secret, provided however, that a contractual or other duty to maintain secrecy or limit use of a trade secret shall not be deemed to be void or unenforceable solely for lack of durational or geographical limitation on the duty").

pre-litigation dispute process, especially considering the relative fragility of trade secrets.¹⁸ Indeed, even where an NDA includes a pre-litigation dispute provision, a disclosing party often will seek a provision that allows it, at any time, to seek a temporary restraining order and preliminary injunction for actual or threatened misappropriation. In contrast, a receiving party may be content with a pre-litigation dispute provision that requires involved efforts to resolve any dispute, disagreement or claimed breach prior to commencing litigation.

Pursuant to a choice of law provision, the parties can specify the State law that will govern the interpretation and enforcement of the contract and the law that will govern a trade secret claim or issue. An informed choice of law decision will account for State law differences on the enforceability of certain aspects of an NDA. As discussed above, some courts applying some States' laws may scrutinize and limit an NDA for anti-competitive effects, just as those courts would scrutinize a non-compete or non-solicitation agreement or provision. A trade secret claim may be brought under federal law, i.e., the DTSA, or state law, i.e., a State's version of the UTSA or New York common law.¹⁹ A trade secret claim generally comprises the same or similar elements under the DTSA, UTSA and New York law, although interpretation and application of the elements can differ according to the jurisdiction and, of course, the facts at issue and certain claims, such as inevitable misappropriation, and remedies may or may not be available under a certain State's trade secret law. Extraterritorial application of the law under consideration can also factor into the choice of law decision.

With respect to a forum and venue selection clause, the primary issue is whether a court, including a jury, or an alternative dispute resolution (ADR) forum, such as an arbitrator, a panel of arbitrators or a mediator, will hear and decide a dispute. Typically, a forum and venue selection clause mandates a single forum and venue for any dispute between the parties that arises out of or relates to the NDA. ADR may be an attractive forum for the receiving party because a claimed breach of the NDA, i.e., alleged bad acts, may be addressed in a confidential environment, such as arbitration, instead of a publicly accessible courtroom. An arbitrator(s) also may be less likely than a court to award injunctive relief. ADR may be an attractive forum for the disclosing party because a confidential environment, such as arbitration, makes it easier to maintain the secrecy of any asserted trade secret. At the same time, the disclosing party may want a judge and jury to hear and decide its misappropriation case. Of course, depending on the goals, circumstances and experience of each respective party and the nature of the interaction or transaction at issue, a given party's preference for a certain forum may run counter to those general expectations. Another factor to consider is a party's familiarity with a particular forum and the forum's overall experience and body of case law relating to trade secret misappropriation. Finally, where the parties are domiciled and, in particular, the locations from which they operate also may factor into reaching an agreement on a forum and venue selection clause. One party may not wish to litigate a misappropriation case on the "home court" of the other party, where the jury's and perhaps even the judges' familiarity with a party may create a "home court" advantage.

Commented [14]: Case cites and any elaboration (beyond the durational limits discussed above) would be helpful.

Commented [15]: Same comment as above. Is this scrutiny with respect to trade secrets or confidential information? If a court or State law has equated confidential information with trade secrets for purposes of assessing anti-competitive effects, that would be good to know. As noted, the Commentary is to focus on trade secrets.

Commented [16]: We can further address extraterritoriality issues as part of the choice of law discussion -- i.e., with respect to the DTSA and State law -- and elsewhere, as appropriate, such as in connection with the forum selection clause discussion (TTC).

Commented [17]: Is there support for this proposition?

¹⁸ *Kinship Partners, Inc. v. Embark Veterinary, Inc.*, 3:21-cv-01631-HZ, at *17 (D. Or. Jan. 3, 2022) ("A trade secret once lost is, of course, lost forever.")

¹⁹ The UTSA has been adopted in one form or another by 49 States, with the only exception being New York, and by the District of Columbia.

Other Documents

In addition to an NDA, there are other documents that may be negotiated and exchanged between parties prior to sharing trade secrets. These documents may include (a) policies and procedures for employees of, or other individuals affiliated with, the receiving party who are authorized to access shared trade secrets and (b) as discussed above, acknowledgments, signed by those employees or other individuals, in which they acknowledge and agree to be bound by the NDA and accompanying policies and procedures.

The parties also may enter into agreements that protect against unfair competition, such as non-competition or non-solicitation agreements. Non-competition agreements may proscribe the receiving party from engaging in certain competitive activity or lines of business while it possesses or can access the disclosing party's trade secrets and for a period thereafter, which period may be based on or a proxy for an independent development period. Notably, if there is a dispute, the receiving party may and likely will argue that such a period is the maximum duration of any injunctive relief the disclosing party can seek and obtain. Non-solicitation agreements may proscribe the receiving party, or both parties, from soliciting and hiring key employees of the other party within a certain period. Key employees authorized to acquire, access, disclose or use shared trade secrets also may enter into non-competition or non-solicitation agreements. There may be antitrust considerations regarding certain types of anti-hire provisions that the parties should be aware of when crafting these types of provisions.

Finally, before sharing any trades secrets, the disclosing party and receiving party should each determine whether it is a party to any existing contract that prohibits or limits the contemplated trade secret sharing or needs to be accounted for in structuring the sharing and any subsequent relationship. Such a contract, if it exists, may be with a third party. Existing contracts with individuals, such as employees or agents, especially those employees or agents who will be involved with the trade secret sharing, also may be relevant. An overall goal is to enter an NDA that is consistent with relevant, existing contracts and that avoids any conflict with or breach of relevant, existing contracts.

2. **PHYSICAL TOOLS**

Physical tools are tangible, often readily visible measures, such as notices and barriers, for protecting trade secrets.²⁰ A disclosing party, such as a trade secret owner, often uses physical tools to protect its trade secrets in the normal course of business. At the pre-due diligence or pre-relationship stage, the disclosing party will not likely share identified trade secrets. So, at this stage, physical tools that the receiving party will have to use during due diligence or a relationship – when the receiving party acquires, accesses, discloses and uses shared trade secrets -- can be investigated and assessed and then specified in the NDA. Such pre-sharing investigation, assessment and specification can include the disclosing party informing the receiving party of the disclosing party's physical tools that will need to be implemented by the receiving party. Such pre-sharing investigation, assessment and specification can reduce the risk of physical tool deficiencies, mistakes or failures, which can

²⁰ See note 4, *supra*.

Commented [18]: We should clarify this statement. This statement seemingly applies to the receiving party's key employees and suggests that he/she/they will enter into noncompetes that benefit the disclosing party? Any noncompete entered into by the disclosing party's employees would have been entered into before the pre-sharing phase and those noncompetes would not seem to be a legitimate concern of the receiving party, unless, e.g., the receiving party later solicits or hires the disclosing party's employees.

Commented [19]: Restrictive covenants can be a tricky area -- esp as to noncompetes. We need to develop this discussion a bit further and should at least note with citations that certain States have banned or limited noncompetes, but have also been careful to recognize trade secrets as a protectible interest. There may be an opportunity here to cross reference to the Employee Life Cycle Commentary, as I believe noncompetes are addressed there -- w/t/ employees, yes, but still a likely relevant discussion. Likewise, we need to develop the anti-trust angle further.

Commented [20]: This section is pre-due diligence/pre-relationship. Under the circumstances of 2 parties trying to understand if a transaction or joint development between 2 separate companies would be worthwhile, there necessarily needs to be some sharing of information. Not the entire list of detailed trade secrets, but this should be a discussion of initial exchanges of information and how that should be protected.

negatively impact an asset's trade secret status. In some situations, the disclosing party may want the right to inspect and approve and require supplementation or modification of the receiving party's physical tools to further reduce that risk and avoid any misunderstanding, ambiguity or conflict.

There are multiple physical tools available. The use of any physical tool depends on the circumstances at issue and there often is a relatedness or overlap between contractual, physical and technological tools.²¹ For example, a physical document may be physically marked as "Trade Secret" or "Confidential," and the same information in electronic form (i.e., electronically stored information (ESI)) may be digitally marked in the same manner. Likewise, a physical document may be stored in a locked room or a locked safe and the same ESI may be password-protected and stored on a local hard drive in a locked room. **Examples of physical tools used to protect trade secrets include:**

- Mark protected information with express, conspicuous labels, watermarks or legends with text such as "Trade Secret" or "Confidential"
- Use tracking devices or **indicia**
- If printing or copying is allowed, print or copy trade secret information on copy-proof or non-photocopyable "paper"
- Use color-coded paper to identify confidentiality, or different colored paper for different levels of confidentiality, for the information thereon
- Transport trade secrets via secure carriers and using locked, secure containers
- Building Security
 - Secure trade secrets in one or more of locked drawers, filing cabinets, safes or rooms
 - Mark areas containing trade secrets as "confidential" or with a similar designation
 - Control and restrict access to those marked areas
 - Store trade secrets in offices or other rooms with doors, rather than cubicles or open spaces
 - Maintain trade secrets information in windowless rooms
 - Provide secure work areas where trade secrets can be accessed, reviewed and used without exposure to others who are not authorized to access or use the trade secrets
 - Maintain access logs for anyone entering a secure area where trade secrets are stored or used
 - Require key card or code access for employees, including levels of permission, especially for secure areas
 - Install gated, perimeter fences to keep out uninvited, unscheduled or uncontrolled visitors
 - Install video surveillance cameras to monitor ingress and egress to the facility, building or secure areas, such as where trade secrets are stored, used, embodied or in operation
 - Install alarm systems
 - Install bars on windows

²¹ Protective measures, i.e., all contractual, physical and technological tools, typically are considered together in assessing whether the measures have been reasonable. A disclosing party can, of course, evaluate particular tools, such as physical tools, for reasonableness. Further, where trade secrets are to be shared, an evaluation of overall or specific tools should include the disclosing party's tools and the receiving party's tools.

Commented [21]: Let's get case law to support the footnote.

Commented [22]: Most, if not all of these suggestions are for due diligence or relationship. They seem or may be too stringent to require before due diligence or a relationship.

Commented [23]: Let's clarify how this is not a technological tool.

- Employ security guards and dogs to verify and admit visitors at facility, building or secure area entrances and patrol the grounds during and after business hours
- Visitor Protocols
 - Maintain logs of visitor entry and exit
 - Require visitors to be identified and badged when on premises
 - Require visitors to sign agreements not to access/acquire/remove Company information without permission
 - Escort visitors while in the facility, building or secure areas
 - Search visitor bags when entering and exiting the facility, building or secure area
 - Prohibit recording of any audio and video and taking of any photographs during visits by, e.g., collecting devices with any recording capability, such as a camera, and affixing security tape to cover any camera lens
- Incident Response Plan to address actual or potential trade secret misappropriation, including any unauthorized, access, acquisition, disclosure or use or related events or issues
- Employee training and policies
 - Employee Manuals, Policies and Guidelines for trade secrets, in printed or ESI form, distributed to employees with signed and dated acknowledgement of reading, understanding and receipt
 - Explain what trade secrets are (without disclosing any trades secrets) and how they are marked and different from confidential information
 - Explain with whom you can discuss trade secrets and to what extent
 - Treatment of a third party's trade secrets, including segregation from the Company's trade secrets
 - Where and how to store trade secrets, including securely storing lab notebooks in, for example, a locked area or desk, and password protecting an e-lab notebook, any not leaving the lab notebook unattended on a desk or opened on an unattended laptop, tablet or other device
 - Travel protocols, such as using privacy screens on approved or issued travel devices, including laptops and tablets, not leaving any devices unattended or unsecured and not taking trade secrets with you
 - How to dispose of a copy of a trade secret, through, for example, shredding or deleting, when no longer needed or access is terminated
 - Secure trade secrets when off-site, including when at home, working remotely or traveling, if such activity is permitted (i.e., locked office, locked filing cabinets)
 - Return or destruction of trade secrets where access, or need to know, is terminated
 - Return of trade secrets upon employment termination or furlough, whether voluntary or involuntary
 - Obligations under and responsibilities and roles in, incident response plan, including procedures for timely reporting any actual, potential or suspected (i) breach of a policy or procedure for protecting trade secrets or (ii) unauthorized access, acquisition, disclosure or use of a trade secret

- Training new or returning employees and periodic refresher and updated training for existing employees²²

3. TECHNOLOGICAL TOOLS

Like physical tools, technological tools can be key means for protecting many trade secrets.²³ A disclosing party, such as a trade secret owner, often uses technological tools to protect its trade secrets in the normal course of business. At the pre-due diligence or pre-relationship stage, the disclosing party will not likely share identified trade secrets. So, at this stage, technological tools that the receiving party will have to use during due diligence or a relationship -- when the receiving party acquires, accesses, discloses and uses shared trade secrets -- can be investigated and assessed and then specified in the NDA. Such pre-sharing investigation, assessment and specification can include the disclosing party informing the receiving party of the disclosing party's technological tools that will need to be implemented by the receiving party. Such pre-sharing investigation, assessment and specification can reduce the risk of technological tool deficiencies, mistakes or failures, which can negatively impact an asset's trade secret status. In some situations, the disclosing party may want the right to inspect and approve and require supplementation or modification of the receiving party's technological tools to further reduce that risk and avoid any misunderstanding, ambiguity or conflict.

Importantly, the use of technological tools assumes that the disclosing party agrees to electronically share trade secrets. A disclosing party may agree to share one or more trade secrets, at least initially, only in physical, or paper, form in a secure physical location where contractual and physical tools are utilized. Under such circumstances, the use of technological tools may not be necessary.

A disclosing party should be well prepared, based its own operations and technological tools, to specify the technological tools the receiving party needs to implement or utilize. Indeed, in the modern, remote world, trade secrets often are electronically created, stored, acquired, accessed,

²² See, e.g., *MicroStrategy Inc. v. Business Objects, S.A.*, 331 F. Supp. 2d 396, 403, 420 (E.D. Va. 2004) (finding MicroStrategy "took reasonable steps to preserve the secrecy of its information" by having, among other things, "physical security, such as locked doors, limited access to its buildings through the use of badges, and the use of security cameras"); *U.S. v. Shanshan Du*, 570 Fed. Appx. 490, 500 (6th Cir. 2014) (reasonable measures included physical security such as "a locked facility monitored at all times by security guards, who required employees to show a photo identification to enter ... guards checked all bags and computer devices carried out of the building, patrolled the facility after hours, and escorted visitors within the facility"); *U.S. v. Hanjuan Jin*, 883 F. Supp. 2d 977, 998-999, 1008 (N.D. Ill. 2012) (reasonable measures included security officers, cameras, alarms, gated car access with key card); *Smithfield Packaged Meats Sales Corp. v. Dietz & Watson, Inc.*, 452 F. Supp. 3d 843, 858 (reasonable measures included physical security such as "codes, badges, or fobs to access its physical offices and plants, and requir[ing] visitors to sign agreements preventing them from removing information from offices and plants"). See also *1 Corp Couns Gd to Tech Mgmt & Trans* § 6:1, 6:14 -6:24; PowerPoint from USPTO website with some physical security measures: [Microsoft PowerPoint - 7 Steps to Protecting Your Trade Secrets short version for dissem \(uspto.gov\)](#)

²³ See note 4, *supra*.

disclosed and used by a disclosing party.²⁴ That electronic activity occurs on and through a variety of systems, equipment, devices and media, such as proprietary databases, shared folders and drives, cloud systems, email and other communication platforms, portals, such as VPNs, on-site computers and remote computers including laptops, tablets and smartphones. The disclosing party's awareness of its trade secret-related electronic activity, systems, equipment, devices and media, as well as the corresponding technological tools it utilizes, should significantly inform its technological tool requirements for the receiving party.

For example, a disclosing party may have to decide whether to provide the receiving party access to its platform or portions thereof. If such access will be provided, then the disclosing party can determine the credentials needed to gain access and the manner in which, including the device through which, access will be permitted. Where appropriate and possible, the disclosing party also can test or conduct a dry run to ensure the protocol for access functions properly and to identify and troubleshoot unanticipated or overlooked vulnerabilities or risks.

Overall, the disclosing party can keep in mind four important platform-related issues: (1) whether the platform is sufficiently secure, such that trade secrets can be shared with minimal risk of misappropriation by unauthorized entities or individuals affiliated with the receiving party or by entities or individuals not affiliated with the receiving party, (2) whether the platform is configured to allow access to trade secrets on only a "need to know" basis, i.e., to only authorized individuals,²⁵ (3) whether the platform is configured to allow access on only certain days and at only certain times and (4) whether the platform is configured to monitor who accessed what trade secrets, when and by what means and to monitor other activity, such as downloading and printing, assuming such other activities, or functions, are enabled and permitted.²⁶ Addressing those issues before sharing trade secrets can help ensure that those measures properly will be implemented when the trade secret sharing takes place.

Importantly, the disclosing party can consider and address essentially the same four issues if it will be establishing a data or due diligence room – including one that is or includes a clean room – for trade secret sharing. Such rooms are further discussed below.

There are multiple technological tools that a disclosing party can use to protect trade secrets that are in electronic or digital form. Some of those tools can be used or inform the tools to use when protecting shared trade secrets. Those tools that a disclosing party can use include:

- Password protect documents, files, folders and devices that are or contain trade secrets
- Encrypt documents, files, and folders that are or contain trade secrets
- Transmit trade secrets via encrypted communications

²⁴ Trade secrets that are electronically stored are created, stored, acquired, accessed, disclosed and used by the disclosing party are also subject to technological threats.

²⁵ Failing to limit trade secret access to only those individuals who "need to know" the trade secrets in connection with the due diligence or relationship can be evidence that the trade secrets were not reasonably protected. [Case cite]

²⁶ Such monitoring may produce key evidence in a subsequent trade secret misappropriation or breach of contract dispute.

- Encrypt devices, hard drives and memory devices where a trade secret is stored
- Maintain computer logs that track who accessed a trade secret, or if segmented, a portion of a trade secret, by, name and date and time of log in to and log out of the platform, for example, and date and time of access in to and access out of a file, folder and network
- Maintain computer logs tracking the device used to access a trade secret or a portion thereof
- Maintain computer logs of any trade secret downloading, uploading, copying, printing, attaching, e-mailing or otherwise sending, saving or saving as, and revisions and deletions, bearing in mind that all such functionality should be permanently disabled where possible
 - Generate alerts on detection of an abnormal volume of downloading, printing, e-mail traffic, including forwarding, or revision or deletion of a trade secret, optionally with threshold generating interruptions
- Require complex passwords with frequent change intervals and password storage protocols, including storage in physically secured drawers or encrypted virtual password lockers
- Using two or multifactor authorization technologies to access a trade secret
- Limit remote access to the computer network, platform, folders or files that are or contain a trade secret
- Allowing access to a trade secret only from authorized devices, such as company-issued desktops, laptops and tablets
- “Fingerprinting” documents and files with a “marker,” such as a typographical error or other benign error or content, to more easily prove trade secret misappropriation or breach of contract if that ever becomes necessary
- Disable data ports on computers to prevent downloading or uploading trade secrets onto remote memory devices or other memory or storage medium
- Ensure vendors and other business partners implement and comply with protective measures
- Cyber-security protocols
 - Quarantine excessive email traffic
 - Limit access to social media accounts
 - Limit access to unauthorized websites
 - Update malware and anti-virus software
 - Include, in Incident Response Plan, a response to an intrusion attempt and cyber attack
- Secure and effective erasure of trade secrets in magnetic memory after need for that copy has ended or memory is redeployed
- Maintain trade secrets on computers or servers physically disconnected from internal or external networks
- Limit sharing of source code to secure third-party escrow services, with strict access controls, and limits on downloading, copying or printing²⁷

Commented [24]: Do biometrics deserve mention or analysis?

Commented [25]: Is the source code a specific trade secret, or does it include specific trade secrets, or is this a suggested broad step to be taken for all source code so nothing is missed?

²⁷ See 1 Corp Couns Gd to Tech Mgmt & Trans § § 6:1, 6:14 -6:24; PowerPoint from USPTO website with some physical security measures: [Microsoft PowerPoint - 7 Steps to Protecting Your Trade Secrets short version for dissem \(uspto.gov\)](#).

V. Considerations When Conducting Due Diligence Or In A Relationship

A. IDENTIFY ASSETS AT ISSUE

[Proposed] Principle No. 2: A trade secret owner should identify a trade secret when it is shared as part of efforts to protect the trade secret and to realize an appropriate economic return on the trade secret.²⁸

[Proposed] Principle No. 4: As the parties' interaction progresses from pre-due diligence to due diligence or a relationship, the disclosing party should periodically update the categories of trade secrets that are to be shared, specify the identified trade secrets that are shared, specify the identified trade secrets that are retrieved by the disclosing party or that are returned or destroyed by the receiving party and update, as appropriate, the entities and individuals who can or cannot acquire or access the shared trade secrets.

Issue No. 1: If a trade secret is not properly identified when shared, then potential consequences are:

- (a) the subject of the disclosing party's (e.g., trade secret owner's) and receiving party's protective efforts does not legally exist and trade secret status is lost,
- (b) the receiving party lacks notice of the trade secret requiring protection, thereby resulting in compromised secrecy and potential loss of trade secret status,
- (c) an inaccurate valuation of the trade secret and, as a result, a lower economic return on the trade secret,
- (d) less control over, and reduced ability to track, the receiving party's use and disclosure of, provision of access to and, post-due diligence or post-relationship, return or destruction of the trade secret,
- (e) inadvertent sharing of other information, including other trade secrets. In other words, a disclosing party should not disclose more than necessary and a receiving party likewise should not want to receive more than necessary. Corresponding concerns include loss of trade secrecy status for inadvertently disclosed trade secrets and potential exposure to claims that were not contemplated, respectively,

Commented [26]: Perhaps too detailed for a Principle, but concepts are sound. Suggestion is to streamline and integrate specifics into the body of the Commentary.

²⁸ The Sedona Conference Commentary on the Proper Identification of Asserted Trade Secrets in Misappropriation Cases substantively analyzes the standard for proper trade secret identification, i.e., sufficient particularity, and provides examples of proper trade secret identification. Some of that earlier Commentary, including its principles and recommendations, are accounted for in this Commentary.

(f) difficulty in identifying, or failing to identify, joint developments or modifications and corresponding rights and interests and

(g) difficulty in pursuing a trade secret misappropriation claim against the receiving party or a third party.

[Proposed] Guidance No. __:

Part of the identification process can include the receiving party identifying its related or similar trade secrets, communicating and verifying that it possessed the disclosed trade secret prior to disclosure and separating pre-existing or ongoing work from the parties' relationship.

[Proposed] Guideline: At the time of identification, a disclosing party should consider implications of a prior commercial use defense under 35 U.S.C. § 273.

Issue No. 2: If a trade secret is not properly identified when shared, then a potential consequence is increased difficulty in proving, by clear and convincing evidence, a prior commercial use defense under 35 U.S.C. § 273 and, in particular, the subject matter to which the defense applies.

[Proposed] Guideline: The receiving party should confirm the disclosing party has reasonably protected the shared trade secrets and not transferred any trade secret rights (outright or to derivative works) to another person.

1. IDENTIFICATION OF TRADE SECRETS SHARED

The transition from pre-due diligence or pre-relationship to due diligence or a relationship typically warrants a correspondingly heightened protocol for sharing trade secrets, as opposed to sharing a list of categories or general subject matter of the trade secrets and that may have been provided pre-due diligence or pre-relationship. In other words, trade secrets likely were not, and should not have been, shared before due diligence or a relationship. During due diligence or a relationship, trade secrets will be shared and corresponding identification obligations of the disclosing party and confidentiality obligations of the receiving party will need to be fulfilled for the due diligence or relationship to proceed.

Having said that, once due diligence or a relationship commences, existing obligations set forth in a prior agreement, such as a confidentiality or non-disclosure agreement (NDA), may not cease. Rather, all or some obligations may continue, to the extent sufficient and applicable, or they may be modified or enhanced while accounting for the parties' focus on the commercial objectives of the due diligence or relationship and recognizing that a transaction, for example, may or may not come to fruition, change, evolve or terminate. Continuing obligations may arise, for example, where a triggering event or condition in a prior agreement occurs or is satisfied. Modified or enhanced obligations may be set forth in a new agreement or in an addendum to a prior agreement.

As noted in Section IV, there are three major categories of protective measures for trade secrets before, during and after due diligence or a relationship: (1) contractual tools; (2) physical tools;

Commented [27]: Walmart Inc. v. Cuker Interactive, LLC, 2020 U.S. App. LEXIS 4289, **10-12 (8th Cir. Feb. 12, 2020) is a good case to consider/account for w/t the due diligence or relationship phase, esp. w/t trade secret identification and its connection to protective measures.

and (3) technological tools. Trade secret owners should consider utilizing all three types of tools when protecting trade secrets during due diligence or a relationship. While tools can be organized into those three categories for ease of discussion, the different tools are, in practice, connected.

Principle No. V-1 - When parties are engaged in due diligence or a relationship that involves sharing trade secrets, the disclosing party should share only trade secrets in the agreed-upon categories or, if the parties have not previously agreed in writing on a category into which a to-be-shared trade secret falls, then previously agreed to categories should be supplemented prior to disclosing the trade secret and the disclosing party should identify the shared trade secrets with sufficient particularity.

At the inception of due diligence, a disclosing party should possess a list of identified trade secrets it intends to share and know the tools that have been or will be implemented by the receiving party to protect the trade secrets. To be clear, a due diligence or relationship list of trade secrets, as opposed to a pre-due diligence or pre-relationship list of a list of categories or general subject matter of trade secrets, can include the identified trade secrets. Alternatively, the identified trade secrets may be an addendum to the due diligence or relationship trade secret list, with such an approach potentially facilitating more controlled disclosure of, access to and use of the shared trade secrets.

Principle No. V-2 -- When parties are engaged in due diligence or a relationship that involves sharing trade secrets, the parties should use tools to protect shared trade secrets, and the tools that the receiving party must use should be specifically enumerated in a contract, such as an NDA.

A common starting point, or first tool, for protecting trade secrets during due diligence or a relationship is a contract, such as an NDA, that limits access to and use of trade secrets. As noted above, this NDA may be a continuation of or build upon an existing NDA. Notably, an NDA used in connection with due diligence typically will limit disclosure of, use of and access to any shared trade secret to only evaluation of a possible future relationship. Further, an NDA used in connection with due diligence or a relationship typically accounts for physical tools and technological tools to protect trade secrets shared during due diligence or a relationship.

The NDA often addresses both written and oral disclosures of trade secrets. Oral disclosures may occur during, for example, an interview or meeting relating to the due diligence or relationship. Such disclosures typically can be memorialized through a procedure in the NDA, with such procedure allowing for a post-disclosure written identification of the information designated as a trade secret. Other oral disclosures may occur outside a scheduled interview or meeting. For example, a receiving party may seek and a disclosing party extemporaneously may provide supplemental or clarifying information because of human error, i.e., a trade secret may have been insufficiently identified when initially disclosed. Regardless of the circumstances, an oral disclosure may be subject to differing interpretations or recollections. So, as a general proposition, oral disclosures should not be seen as a preferred method of sharing and when they do occur, they should be promptly and accurately converted to a written disclosure pursuant to the agreed upon procedure.

Pursuant to the NDA, progressive incremental disclosure can be an appropriate approach. Under this approach, trade secret sharing will be gradual and contained. For example, only trade secrets in a certain category or categories initially will be disclosed, only a representative trade secret or trade secrets initially will be disclosed, only a very limited number of persons initially will be

Commented [28]: The Walmart case also applies here, as it ties identification to protective measures. Additionally, we can address in this section (does not need to be included in the Principle) a Schedule For Potentially Sharing Additional Trade Secrets.

Commented [29]: We can/should further develop the trade secret identification step by addressing any practical or unique aspect to trade secret identification in a due diligence or relationship setting. Perhaps things like prosecution bar, etc. The standard for proper identification is in a separate Commentary, which is cross-referenced in this Commentary. The issues/aspects to consider here are those that arise out of or flow from sharing properly identified trade secrets.

Commented [30]: Ideally, we avoid promoting/citing to the ABA or other bar association, organization or group in the body of (as opposed to a footnote in) the Commentary. Our overall goal is original content/thought based on case law and experience, with attribution where appropriate, of course. Also, the written vs. oral disclosures is a great topic to meaningfully address, i.e., beyond just a reference. Yes, there will always be some oral disclosures, whether through interviews or otherwise. But that does not make the practice desirable, especially if the only disclosure of a trade secret or a key part of a trade secret is an oral disclosure. No prior or contemporaneous written record of a disclosure can create problems, including a risk of or actual loss of rights. And, yes, the "everything we disclosed during yesterday's meeting was a trade secret" is something we can and should address/critique.

authorized to access the disclosed trade secrets and time constraints will be placed on stages of access, review and evaluation of the disclosed trade secrets. Then, if mutual interest in continuing the process towards, for example, a relationship exists, the disclosure can incrementally progress to greater disclosure and access. Alternatively, progressive incremental disclosure can allow parties to more easily terminate the due diligence and separate.

Confidentiality obligations in an NDA often are mutual. That two-way street accounts for the reality of information sharing. In other words, during due diligence or a relationship, a disclosing party often becomes a receiving party and vice versa. For example, the receiving party, prior to receipt of a trade secret from the disclosing party, may have conducted its own research or development relating to information it receives. In order to establish its rights and interests, the receiving party will share its information with the disclosing party. The receiving party also may have third-party obligations that require it to obtain mutual NDA obligations. Thus, while due diligence or a relationship initially may focus on rights and obligations that protect a disclosing party's trade secrets, there often is a need for corresponding rights and obligations to protect the receiving party's trade secrets that also are shared during the due diligence or relationship. See *Edifecs Inc. v. TIBCO Software*, 756 F.Supp.2d 1313 (W.D.Wash.2010); *Big Vision*, 1 F. Supp.3d 224.

Mutual sharing of trade secrets or related information also is likely – and corresponding protections are therefore appropriate – where new trade secrets may be jointly developed or existing trade secrets may be modified. See *Big Vision Private Ltd v. E.I. DuPont de Nemours & Co.*, 1 F. Supp.3d 224 (S.D.N.Y. 2014), *aff'd* 610 Fed. Appx. 69 (2nd Cir. 2015) (trade secret owner unable to enforce alleged trade secrets because it failed to give potential joint venturer, who also had been developing technology in the same area, clear notice of trade secrets shared).

Importantly, confidentiality obligations relating to shared, jointly developed or modified trade secrets can continue where due diligence ends without a subsequent relationship, such as a licensor-licensee relationship, or where the subsequent relationship terminates. Unsurprisingly, a receiving party often seeks to limit the duration of confidentiality obligations and, in effect, put a shelf-life on the trade secrets at issue. Such limitations typically conflict with the desire of a disclosing party, such as a trade secret owner. The disclosing party often wants confidentiality obligations to continue in perpetuity or until the trade secret becomes generally or publicly known through no fault of the receiving party. Sometimes there is room for compromise as to certain trade secrets. For example, a trade secret may have a natural shelf-life because it will be publicly or generally known when executed (e.g., a marketing plan) or comprises data (e.g., cost or pricing data) that is time-sensitive, meaning data that will lose its value or becomes stale as time passes and market conditions change.

During due diligence, information frequently is shared through a data room. Depending on the limitations on access to the room and the information, including documents and files, stored in the room, a data room may be or can include a clean room. Whether one is considering a physical, i.e., in-person, virtual, i.e., remote or combined physical and remote data room for information review, a data room with trade secrets can include the following protections:

- A mutually acknowledged inventory of the trade secrets in or available in or from the data room.
- Passwords to access electronically stored information (ESI), with an additional password to access trade secrets.

Commented [31]: This concept (progressive, incremental disclosure) is sound, and should be addressed and developed. Great opportunity here for a suggested provision or portion of a provision for the appendix, informed by real world/practical considerations. For example, a relationship may be appealing w/r/t certain categories of trade secrets and not others; the trade secrets in the 2nd and 3rd categories, e.g., may not need to be disclosed because the potential buyer says category 1 is all I want or the buyer may say I don't like or want any of what you're selling and I'm completely out. Also, the parties' mutual trust and confidence – or at least the disclosing party's trust and confidence – needs to exist or is at least desirable to some extent. As a practical matter (our end game), how is either established, measured or eliminated in these situations?

Commented [32]: Important topic, and can be tied into the typical carve out for trade secrets – which excludes, e.g., independent development of subject matter or subject matter already and verifiably in the possession of the receiving party. Mutual confidentiality obligations can impose a real-time obligation on the receiving party; for example, within x days of receipt, the receiving party must notify the disclosing party that subject matter labeled as a disclosing party's trade secret is subject matter the receiving party already and verifiably has.

Commented [33]: We need to clarify the parenthetical/what this case actually addresses and this is another great opportunity for a clause in the appendix.

- Restrictions on communication or sharing and storage of passwords and requirements to periodically reset sufficiently strong passwords.
- Physical locks, key cards and sign-in/sign-out sheets in any physical setting.
- Each file or document constituting or containing trade secrets should be expressly and conspicuously marked as “TRADE SECRET” or otherwise. Such marking can include a watermarked notice or header on each document or file, as well as a pop-up message that alerts the viewer the document or file about to be accessed constitutes or contains a trade secret and requests confirmation, through a click or box-checking, that he or she is authorized to access the document or file and agrees to or confirms all corresponding obligations.
- Trade secrets should not be downloadable, attachable, printable or editable from or in a virtual data room, nor physically removed from a physical data room.
- A data room should be free of all unauthorized devices, including smartphones, tablets and laptops, with any wifi, memory, communication (e.g., e-mail, texting, instant messaging and telephonic) capability and recording (e.g., audio, video and photographic) capability.
- ESI in a data room is stored locally, e.g., on a desktop without wifi or internet connection or access.
- Access to any trade secret is continually monitored and logged, with records for each document or file showing when it was viewed, by whom, and for how long.
- Physically accessible locations should be under video surveillance.
- Access to trade secrets or parts of trade secrets may be sequenced or segmented so that trade secrets or parts of trade secrets may be viewed only during the late stages of the due diligence or at certain points in a relationship.
- No single person is allowed to access all trade secrets, each person’s authorization to access trade secrets is confined to certain categories, or sub-categories or silos, of trade secrets or certain trade secrets.

2. IDENTIFICATION OF TRADE SECRETS OR OTHER ASSETS MODIFIED OR JOINTLY DEVELOPED

Just as pre-due diligence or pre-relationship protective measures, or tools, can and likely will be enhanced as the parties transition into due diligence or a relationship, protective measures, or tools, can and likely will be enhanced as the parties transition into a post-due diligence relationship. Mutual protections in effect during due diligence or a relationship generally can continue, perhaps with appropriate modifications, into a post-closing relationship. Due diligence generally includes a disclosure, review and inquiry model of communications. Development work, on the other hand, is

Commented [34]: Do we want to address file names and the pros/cons of file names that include or do not include “Trade Secret” or “Confidential”? Those terms in file names may serve a notice function and may also facilitate theft by a dishonest insider or hacker who is looking for the most easily found and/or most valuable information. To be clear, file names are separate from marking the actual document or file. Also, a generic file name seems just as beneficial (no dinner bell) as including trade secret in the file name (more/reminder notice to those authorized to access the trade secret).

Commented [35]: Whether this prohibition is realistic has been raised. Thoughts?

Commented [36]: Whether this prohibition is realistic has been raised. Thoughts?

Commented [37]: We should address note-taking by any reviewing person. Is note-taking allowed? Realistically, it creates a risk because control over the trade secret or a part of it is lost. If allowed for some reason/purpose or under some circumstances, are copies of the notes provided to the trade secret owner as a matter of course, by request or under certain, triggering circumstances?

Commented [38]: Whether this prohibition is realistic has been raised. Thoughts?

best supported by an iterative process involving suggestion and collaboration in addition to disclosure, review and inquiry.

Where trade secrets are shared, related research, development and engineering efforts may take place. Sometimes those efforts are joint efforts and sometimes those efforts are independent, parallel efforts. Regardless of who undertakes those efforts, modifications, including improvements, to a trade secret and subject matter derived from a trade secret are topics that can be addressed in an agreement that governs the parties' current relationship.

A key issue to address when it comes to modifications or derivations is who owns the modifications to and subject matter derived from a trade secret, whether jointly developed or not. Parties can agree to joint ownership, where each party owns an undivided interest in the subsequently developed asset, with the right to sub-license. Alternatively, parties can agree to a licensing arrangement, where one party is the owner/licensor and the other party is a licensee. An important step in assessing whether an asset is a subsequently developed asset is a complete and accurate list and identification of the trade secrets that each party has shared with the other party. Notably, listing and identifying what is not being shared or included in a relationship can be just as important as listing and identifying what is being shared, especially if the parties' relationship, and corresponding agreements, have evolved from pre-due diligence to due diligence to post-closing relationship. Additionally, there can be disclosure obligations such that the party first aware of the subsequently developed asset discloses it to the other party. Such an obligation can be buttressed with corresponding audit and inspection rights.

Principle No. V-4 – When parties are engaged in a relationship that will involve sharing trade secrets and may involve modifications to those trade secrets or jointly developed trade secrets, the parties should agree in writing on procedures, and a process for amending procedures, for (i) identifying, designating and communicating about any shared, modified or jointly developed trade secrets and (ii) determining ownership of modified or jointly developed trade secrets.

In addition to defining ownership, control, and maintenance of joint trade secrets, define what royalties and accounting will be due, and what inspection and auditing will be available, to the parties, and what will occur upon termination of the relationship.

It is also important to clearly allocate and determine clearly in any joint development agreement or related contracts which party may pursue and own patents or bring enforcement actions as owners of trade secrets. *Lucent Techs., Inc. v. Gateway, Inc.*, 543 F.3d 710 (Fed. Cir. Sep. 25, 2008).

It is important to understand what information each party has or has not contributed to a modified or jointly developed trade secret and when that contribution occurred. Timely disclosure and documentation of a contribution are important to ongoing development work, and to establishing legal rights and interest in and to the results of the development efforts. To that end, parties can update the list and identification of trade secrets shared, modified or jointly developed as the relationship proceeds. Procedures for such updates can be accounted for by contract and can include compliance with such procedures as a precondition to bringing or defending any action relating to a corresponding trade secret.

Commented [39]: Good opportunities to develop examples of provisions or parts of provisions in the appendix.

Commented [40]: Good opportunity to elaborate, clarify and provide examples of provisions or parts of provisions in the appendix.

Commented [41]: Same as prior comment.

Commented [42]: Same as prior comment.

Commented [43R42]: Principle V-4 may be too granular to be a Principle. So, we can/should revise it if it remains a Principle. A big positive is the following is subject matter -- largely set forth in the 3rd paragraph under Principle No. V-4 - - we can include in the appendix as a provision example: "the parties should update and finalize the identification of trade secrets shared developed or modified as the relationship proceeds, and address with one another at the inception of such relationship disclosure requirements for doing so on an ongoing basis throughout the relationship and as a precondition to bringing or defending any action related to such trade secrets"

Parties in a trade secret sharing relationship may find themselves in a trade secret or related dispute. One way to reduce the time and expense of such a dispute is to require timely disclosure and documentation, including periodic updates, of trade secret sharing, modifications and developments, with corresponding audit and inspection rights.

B. PROTECTIVE MEASURES WHEN SHARING TRADE SECRETS

1. Updating Contractual Tools, Including To Track And Control Sharing

- a. Ownership of subsequently developed technology or assets**
- b. Residuals clause**
 - Define “unaided memory”
- c. Audit or Inspection Rights Moving Forward to Ensure Compliance**
 - i. Recipient reporting obligations on protective measures, royalties, sales, access/disclosure/use of the trade secret and return/destruction of the trade secret
 - ii. Compliance with protective measures, royalties, sales, access/disclosure/use of the trade secret and return/destruction of the trade secret
 - iii. Third Party Neutral’s Role, if any

2. Updating Physical Tools, Including To Track And Control Sharing

During due diligence or a relationship, a disclosing party should require that a receiving party use physical tools to protect shared trade secrets.²⁹ In general, those tools should be the same as or similar to the physical tools that a disclosing party was using prior to sharing its trade secrets. Whether the measures taken in a given case will satisfy the legal standard -- reasonable protective measures -- is a question of fact decided on the totality of the circumstances, which may include any standards applicable in the relevant industry and the value or importance of the particular trade secret at issue.

²⁹ The reasonable protective measures requirement accounts for measures taken by a disclosing party, as well as measures taken by a receiving party. *Geritrex Corp. v. Dermarite Indus., LLC*, 910 F. Supp. 955, 961 (S.D.N.Y. 1996) (“Plaintiff must show that it took substantial measures to protect the secret nature of its information.”); *Big Vision Priv. Ltd. v. E.I. DuPont de Nemours & Co.*, 1 F. Supp. 3d 224, 267–69 (S.D.N.Y. 2014) (“There is virtually no contemporaneous documentary or testimonial evidence . . . indicating that Big Vision took *any steps* to ensure the confidentiality of the information it disclosed to third parties.”); *KT Grp. Ltd. v. NCR Corp.*, 2018 WL 11213091, at *13 (S.D.N.Y. Sept. 29, 2018) (citing *Sm. Stainless, LP v. Sappington*, 582 F.3d 1176, 1190 (10th Cir. 2009)) (“[D]isclosure of the alleged trade secrets to individuals or entities who are under no obligation to protect the confidentiality of the information extinguishes the owner’s property right in the purported trade secrets.”); *Nova Chems., Inc. v. Sekisui Plastics Co.*, 579 F.3d 319, 327–28 (3rd Cir. 2009) (holding that information disclosed to defendant distributor pursuant to a license “lost its trade secret status” because the license agreement did not require defendant to “maintain the secrecy of any information it had acquired from [plaintiff]”).

Beyond satisfying the legal standard is marketplace reality. That is, a disclosing party knows, based on its in-house efforts, what physical tools are effective. So, as a practical matter, a disclosing party should not want a receiving party to do less than the disclosing party knows to be effective. Indeed, such a differential may make proving the existence of reasonable protective measures more difficult and may create exploitable or exploited risks that, in fact, lead to the misappropriation of the trade secret and all the corresponding operational and litigation expenses.

- a. Individuals with access; wall off recipient's team conducting a preliminary due diligence; if relationship proceeds past due diligence, individuals with access
- b. Clean room assessment of trade secrets during full due diligence (clean room protocol -- appendix)

3. Updating Technological Tools, Including To Track And Control Sharing

- a. Who accessed the trade secret, or portion thereof
- b. Date of access
- c. Device used to access
- d. Actions, such as downloading, uploading, copying, attaching/sending, saving/saving as and printing³⁰

³⁰ [Possible cross reference to Forensics Commentary.]

VI. Considerations When Ending Due Diligence Or A Relationship

When due diligence or a relationship ends, measures to protect the confidentiality and, thus, the status and value of a shared trade secret must be taken. Some of those measures continue from the due diligence or relationship and some are new measures necessitated by the due diligence or relationship ending. Those measures typically are, and should be, set forth in an NDA or other contract between the disclosing party and receiving party. Generally, both parties will have protective measures obligations, with the disclosing party often focused on the receiving party's compliance with its obligations. That focus often includes the disclosing party seeking confirmation, in action and writing, that the receiving party has met and will continue to meet its obligations. For example, and as discussed above, the disclosing party often will expect and seek (1) return or destruction of the shared trade secrets in the receiving party's possession and (2) the receiving party's written confirmation that those obligations have been fulfilled. A receiving party also may, and likely will, have one or more continuing obligations, such as an obligation to maintain the confidentiality of, and not access, disclose or use, the trade secrets it received. Depending on how the trade secrets were shared and the obligations specified in the NDA or contract, a disclosing party may also expect and seek written verification that (1) any devices, platforms, databases, or repositories that the receiving party possesses or could access are disabled or returned and (2) any data on the devices provided to the receiving party is deleted. A disclosing party should, on its own, account for any written materials, physical materials, such as a prototype or model, and digital or physical credentials, such as usernames, passwords, key cards or badges, that were provided to the receiving party and ensure they are returned, destroyed or disabled. To bolster its protective measures and possibly motivate compliance and reduce the risk of mistakes, deficiencies and failures, a disclosing party also can provide written reminders to the receiving party of its continuing obligations, including confidentiality obligations. A disclosing party also can compare the inventory of trade secrets disclosed to the inventory of trade secrets returned or destroyed to further those same purposes. The inventorying step can be quite important, as it provides an objective data point relating to whether one or more trade secrets are at risk or being misappropriated. Depending on the terms of the NDA or other contract, other measures, such as interviewing receiving party personnel about obligation awareness and compliance and potential risks also may be taken. Notably, such measures are an example of measures that may be seen as not commercially feasible or reasonable, especially by the receiving party, either when the NDA or other contract is being negotiated or when the disclosing party requests such measures without a contractual basis for doing so.

Because of the prevalence of electronic data, human error and even bad intent, the return or destruction of all relevant documents and information may not be possible. But a disclosing party nonetheless should perform the trade secret inventory comparison above and can inventory and examine, forensically if necessary, devices, including smart or cell phones, computers, whether a desktop, laptop or tablet, and any external storage or memory devices, , and online accounts provided to or accessed or used by the receiving party.

Commented [44]: Some clarification is/may be needed here.

The above measures, along with the discussion below, provide a possible framework for a disclosing party to protect its trade secrets when and after a due diligence or relationship ends, whether by its own terms or by termination. A receiving party can also consider this framework as a possible means to facilitate its compliance with its obligations and reduce its risk of committing trade secret misappropriation or breaching an NDA or other contract.

A. POTENTIAL PROBLEMS WHEN ENDING DUE DILIGENCE OR A RELATIONSHIP

As noted above, an NDA, like any contract, may not address every issue and nuance that arises, and that may be especially true where the due diligence or relationship ends. So, many parties can negotiate and agree to provisions that will provide more certainty and better protection -- for the trade secrets and the parties -- when ending the due diligence, as always happens, or ending the relationship, as often happens. Below, we discuss several issues of which parties should be aware when ending due diligence or a relationship and potential ways to address those issues. .

[Proposed] Principle No. 5: Upon the conclusion or termination of the parties' interaction or relationship, the parties should memorialize, in writing, the trade secrets that were shared, the receiving party should return or destroy specified materials, including documents identifying or embodiments of the trade secrets, and the parties should agree on the ownership of and other rights and interests in or to any modified or jointly developed trade secrets or other assets.

1. Failure To Update And Finalize Identification Of Trade Secrets Shared, Modified or Jointly Developed

The disclosing party is responsible for knowing what its trade secrets are and properly identifying them, i.e., setting forth its trade secrets with sufficient particularity, when sharing them with the receiving party. If a receiving party does not understand an identified trade secret, then it can request clarification from the disclosing party, whether or not the NDA or another contract provides a process for seeking and obtaining clarification, amendment or re-definition. If the receiving party does not seek clarification, amendment or re-definition, and a future dispute arises, it unnecessarily may be exposed to liability or greater liability. Depending on the NDA or another contract, the disclosing party may or may not be obligated to clarify, amend or re-define a trade secret upon request of the receiving party. Of course, where a disclosing party has insufficiently or erroneously identified a trade secret, it can and should clarify, amend or re-define the trade secret. If the disclosing party clarifies, amends or re-defines a trade secret, then it should do so in writing, according to any agreed upon protocol, to reduce the risk of and perhaps eliminate a future dispute or improve its chances of succeeding in a future dispute.

Without any request from the receiving party, the disclosing party may itself realize that it insufficiently or erroneously identified a trade secret. Once aware of those circumstances, the disclosing party can and should clarify, amend or re-define a trade secret, whether or not the NDA or another contract provides a process for doing so. As noted above, if the disclosing party clarifies, amends or re-defines a trade secret, then it should do so in writing, according to any agreed upon protocol, to reduce the risk of and perhaps eliminate a future dispute or improve its chances of succeeding in a future dispute.

A trade secret deliberately may be modified during the parties' due diligence or relationship. In other words, the trade secret may be modified not because of a deficiency or error, as discussed above, but to account for a different input, interface or application, for example. Three issues immediately arise and, ideally, all are addressed in the NDA or another contract between the parties. First, is the modification, including who made the modification, the date of the modification and other pertinent details, properly and timely documented? Second, who owns the stand-alone modification, i.e., potential trade secret, and corresponding rights and interests? Third, who owns the modified trade secret and corresponding rights and interests?

Finally, the parties may be in a joint venture or other joint development-based relationship, or joint development may occur as the parties' relationship progresses or evolves. The parties may, through their efforts, jointly develop work product, including a potential trade secret. Like the circumstances where a modified trade secret is at issue, three issues immediately arise and, ideally, all are addressed in the NDA or another contract between the parties. First, is the joint development work, including who performed the work, the date of the work and other pertinent details, properly and timely documented? Second, who owns the jointly developed work product and corresponding rights and interests? Third, if only one party owns the jointly developed work product, does the other party retain any rights or interests?

2. Trade Secrets Not Returned/Destroyed When Due Diligence Or Relationship Ends

Ideally, the parties' NDA or another contract includes a provision obligating the receiving party (1) to return or destroy all the trade secrets it received, (2) to do so upon the disclosing party's written request or fulfillment of another condition, such as termination of the parties' due diligence or relationship, (3) to do so by a certain deadline and (4) to confirm, in writing, to the disclosing party that all such trade secrets have been return or destroyed. In many situations, the receiving party can satisfy those obligations. Indeed, with notice of those obligations in an NDA, i.e., before any trade secrets are shared, the receiving party can take steps to ensure its means of acquisition, access, disclosure and use of the shared trade secrets will not interfere with those obligations.

Having said that, a receiving party may fail to return or destroy all shared trade secrets when due diligence or a relationship ends. Such a failure may result, for example, from (1) a receiving party's lack of technical acumen or ability (2) difficulty in accounting for, or overlooking that, trade secrets may have been routinely backed up and stored in memory the receiving party routinely uses to back up much or all its information, at least temporarily or (3) human error. Such a failure may lead to a dispute between the parties and constitute, for example, trade secret misappropriation or a breach of contract, especially if the parties do not account for the failure in the NDA or another contract and the backed-up trade secrets are not maintained in confidence. So, the parties' NDA or another contract can anticipate and address this failure by, for example, (1) as discussed above, obligating the receiving to confirm that the backed-up trade secrets are destroyed, or permanently deleted, in the normal course of the receiving party's document retention or destruction policy of which the disclosing party has a copy, (2) obligating the receiving party to implement a specific technical solution, if feasible, and (3) specifying remedies for any breach of these obligations. The parties can also include a provision requiring the receiving party to explain, in writing, to the receiving party any asserted justification for any non-return or non-destruction of a trade secret, including return or destruction conflicts with a litigation hold, a trade secret is embedded in an attorney-client communication and part of a corresponding attorney-client privilege claim or a trade secret is embedded in work product and part

of a corresponding work product protection claim. Such an explanation may facilitate a solution, even if delayed, and may reduce the risk of dispute that leads to litigation.

3. Subsequent Work Relating To Trade Secrets Is Performed By The Receiving Party Or Receiving Party Personnel Who Subsequently Work Elsewhere And Perform Work Relating To Trade Secrets

A potentially precarious situation is one where (1) the receiving party engages in its own allegedly independent work relating to the trade secrets, (2) the receiving party enters into a relationship with a third party where they jointly engage in work relating to the trade secrets or (3) receiving party personnel, such as employees, vendors, consultants and independent contractors, who acquired, accessed or used the trade secrets, take a job with a new employer that is engaging in work relating to the trade secrets. Four issues immediately arise: (1) whether the receiving party returned or destroyed all the shared trade secrets, (2) whether the receiving party confirmed that it had returned or destroyed all the shared trade secrets, (3) whether actual trade secret misappropriation, through unauthorized acquisition, disclosure or use, is taking place, and (4) whether trade secret misappropriation, through unauthorized acquisition, disclosure or use, is threatened, including whether such misappropriation is inevitable.³¹ The disclosing party's answers, based on available information, may be (1) we thought so, but now are not sure, (2) yes, but now we do not know if we can trust that confirmation, (3) we believe so, but are not sure and (4) we believe so, but are not sure. To establish and maintain trade secret status for information, the information must be the subject of reasonable protective measures.³² That obligation can be dynamic, meaning, it is tied to the circumstances.³³ Thus, where, as here, the circumstances change, the protective measures may have to be supplemented or upgraded. A first step to reasonably supplementing or upgrading those protective measures may be to promptly notify the receiving party, in writing, of the circumstances and concerns and request confirmation, or re-confirmation, that the receiving party has returned or destroyed all the shared trade secrets and has complied and is complying with all other obligations,

³¹ Inevitable misappropriation is a viable claim in some jurisdictions and not in others. See [REDACTED], p. 1 n.2 (“For example, Illinois and Pennsylvania are two of several jurisdictions that recognize inevitable misappropriation as a form of threatened misappropriation and, as such, as a basis for relief. See, e.g., *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262 (7th Cir. 1995) and *Certainfeed Ceilings Corp. v. Aiken*, Civil Action No. 14-3925, at *4 (E.D. Pa. Jan. 29, 2015). See also *Kinship Partners, Inc. v. Embark Veterinary, Inc.*, 3:21-cv-01631-HZ, at *13 (D. Or. Jan. 3, 2022) (“Several states recognize the inevitable disclosure [*sic*, misappropriation] doctrine under their respective trade secret misappropriation statutes.”) (internal citation omitted); and *id.* (“Seventeen states appear to have adopted the inevitable disclosure [*sic*, misappropriation] doctrine in one form or another.”) (internal citation omitted). California, Colorado, Louisiana, Maryland, Oregon, Virginia and the District of Columbia do not recognize -- and, in some cases, have “specifically rejected” -- inevitable misappropriation as a form of threatened misappropriation and, as such, as a basis for relief. *Certainfeed*, at *4; and *Kinship*, at *13 n.3. As to federal law, the consensus is the Defend Trade Secrets Act (DTSA) does not encompass or provide relief for inevitable misappropriation by an individual. See 18 U.S.C. § 1836(b)(3)(A)(i)(I), (II).”)

³² See note 8, *supra*. See also 18 U.S.C. § 1839(3) (“the owner thereof has taken reasonable measures to keep such information secret”) and UTSA, § 1(4) (ii) (“the subject of efforts that are reasonable under the circumstances to maintain its secrecy”).

³³ *Id.*

including non-use and non-disclosure obligations. A next step, which may be or include initiating litigation, will likely be driven by the receiving party's response or non-response.

As discussed above, the parties may have accounted for some or all of the foregoing circumstances in a pre-litigation dispute provision in an NDA or another contract. The parties also may have specified, in one or more contracts, permissible and impermissible work or other activity, including new or expanded business relationships, after the due diligence or relationship ends, with such provisions addressing, for example, covered subject matter, walling off receiving party personnel and the duration of any restrictions.

- a. Role of restrictive covenants/clauses and other prohibitions to supplement trade secret protection

4. Receiving Party Hires Or Retains Disclosing Party's Present Or Former Personnel

Another potentially precarious situation is one where disclosing party personnel, such as a present or former employee, is hired by the receiving party after due diligence or a relationship between the disclosing party and receiving party ends. Such movement poses a risk that the former receiving party employee will perform work for the receiving party that involves actual or threatened, including inevitable, disclosure or use of the disclosing party's trade secrets. Importantly, the trade secrets at issue may include trade secrets the disclosing party shared with the receiving party and trade secrets the disclosing party did not share with the receiving party. As noted above, a first step for the disclosing party may be to notify the receiving party, in writing, of the circumstances and concerns and request confirmation, or re-confirmation, that the receiving party has complied and is complying with all applicable obligations. A next step, which may be or include initiating litigation, will likely be driven by the receiving party's response or non-response.

Also as noted above, the parties may have accounted for the foregoing circumstances in a pre-litigation dispute provision in an NDA or another contract. The parties also may have specified, in one or more contracts, permissible and impermissible solicitation and hiring practices involving current and former personnel, including employees. Whether non-solicitation or non-competition provisions or other employment-related restrictions are enforceable largely depends on the jurisdiction. For example, non-solicitation agreements are largely unenforceable under California law. Many jurisdictions do not favor non-solicitation agreements. Further, a noncompete for a particular employee may or may not be enforceable. The enforceability of the noncompete can depend on several facts, including the employee's former and new roles, responsibilities and seniority and the trade secrets at issue.

A receiving party can mitigate the risks described above by designing and implementing a strategic onboarding process that includes, for example: (1) obtain and review a copy of any non-confidential restrictive covenant into which the new employee has entered and, as permitted, obtain and review a copy of any confidential restrictive covenant into which the new employee has entered; (2) obtain from the new employee a signed, written verification that (a) the new employee is not violating and will not violate a former employer's rights by accepting and undertaking the new employment, (b) the new employee has fully complied with all return and destruction obligations (e.g., regarding any device, trade secret or other information) of the former employer and (c) the new employee does not possess, on any device or in any tangible (e.g., paper or electronic) form, any trade

Commented [45]: We should further develop this section. The intersection of restrictions on a company/entity and its personnel + trade secrets + anti-trust? Enforceability of such provisions...

Commented [46]: Disclosing party personnel hired away during the due diligence or relationship is another wrinkle to address.

Commented [47]: Non-solicitation agreements, noncompetes and restrictive covenants (as an overall term) should be addressed so we're as complete and clear as reasonably possible. Also, citations/support for this sentence and the next 2 sentences are needed/would be great -- especially cases that account for and catalyze our addressing the trade secret angle to any restrictive covenant.

Commented [48]: Is this clause too broad by referring to a "former employer's rights"?

secret, or other “confidential,” “secret” or “proprietary” information, of the former employer; (3) establish, in writing, the new employee’s obligations to the new employer, including not to disclose or use any trade secrets, or other “confidential,” “secret” or “proprietary” information, of the former employer; (4) ensure the new employee is educated regarding confidentiality, including the new employer’s corresponding policies and procedures; (5) obtain an executed confidentiality agreement between the new employer and new employee; (6) maintain a completed, signed onboarding checklist in the new employee’s file; and (7) ensure the new employee is not performing and does not perform work that involves, or unreasonably risks involving, the former employee’s trade secrets. All the above steps might not be possible, or might not be performed, in a particular company setting. But where a receiving party hires a disclosing party’s employee, the receiving party should balance its resources with the opportunity and need to protect itself.

5. International Sharing Of Trade Secrets

International sharing of trade secrets raises unique issues when a due diligence or relationship ends.³⁴ As an initial matter, proper identification of trade secrets is particularly important where trade secrets are shared internationally, as enforcement can be more difficult. Further, given the rise of economic espionage in an increasingly globalized business world with more frequent cross-border sharing of trade secrets, disclosing parties need a systematic approach to protect their trade secrets and promptly enforce them. Of course, the approach will differ depending on the disclosing party, its resources, the receiving party and the country or countries at issue.

Guideline No. [X]: When sharing trade secrets with a foreign receiving party, a disclosing party should protect its trade secrets and prepare for litigation to enforce its rights.

- a) Discovery is less available for litigation in international forums,³⁵ so a disclosing party must be vigilant in tracking, documenting, and managing any documents and activity relating to sharing trade secrets in case there is a dispute.
- b) Take steps set forth in Section VI(B) to the extent available and applicable to trade secrets shared with a foreign receiving party.
- c) Memorialize, in an agreement with the receiving party, the identification of the shared trade secrets.
- d) Document the return and destruction of trade secrets by the receiving party.
- e) Memorialize, in an agreement with the receiving party, ownership, retention and other rights and interests in and to any modified or jointly developed trade secrets.

Commented [49]: Let’s further develop. Are we saying, e.g., that there is, or the parties should assume there is, no opportunity to identify/define the trade secrets during litigation/dispute resolution in a foreign tribunal?

Commented [50]: Great list. Let’s cross-reference to above sections (as in point b) and further develop any nuance or specific international issue that can be considered or addressed w/r/t each point.

³⁴ For in depth-analysis regarding issues related to international sharing of trade secrets, see The Sedona Conference, Framework for Analysis on Trade Secret Issues Across International Borders, 23 SEDONA CONF. J. 909 (2022).

³⁵ See The Sedona Conference, Commentary on Cross-Border Discovery in U.S. Patent and Trade Secret Cases (May 2021 public comment version).

- f) Ensure compliance with the EU General Data Protection Regulation (GDPR) to the extent applicable.
- g) To the extent it is discovered, or should have been discovered, that trade secrets were or are being misappropriated during the due diligence or relationship but one entity still needs the services of the other for sufficient business reasons, develop a specific strategy to document the disassociation of the parties in a manner to limit, through contractual, physical and technological tools, the receiving party's current and future disclosure and use of the Trade Secrets, while ensuring sufficient time and opportunity to comply with applicable statutes of limitation for a potential misappropriation or other action.³⁶
- h) Consider choice of law and potential forums and venues for any dispute. As discussed in Section IV.C above, parties can include choice of law and forum and venue selection provisions in an NDA or other contract. International trade secret sharing can elevate the importance of these provisions. The different potential forums for disputes all have various costs and benefits for the disclosing party and receiving party.³⁷
- i) Regarding points a and h above, U.S. Courts increasingly offer a favorable environment for companies to pursue trade secret misappropriation claims against foreign defendants. U.S. Courts interpreting both the Defend Trade Secrets Act and some state versions of the Uniform Trade Secrets Act are permitting extraterritorial misappropriation claims.³⁸ But given the difficulty of obtaining foreign discovery, potential personal jurisdiction issues and enforcing any remedy, disclosing parties, i.e., potential plaintiffs, need to be well organized in collecting

³⁶ Ping-Hsun Chen, TRADE SECRET PROTECTION AGAINST MISAPPROPRIATION COMMITTED BY YOUR FOREIGN DISTRIBUTOR-A LESSON FROM ATRICURE, INC. V. JIAN MENG, 102 J. Pat. & Trademark Off. Soc'y 252, 263 (2022).

³⁷ For in depth-analysis of issues relating to the forums and legal regimes chosen for disputes over internationally shared trade secrets, including various U.S. State Courts, U.S. District Courts, the U.S. International Trade Commission, the Economic Espionage Act of 1996, regulatory actions and the World Trade Organization's Agreement on Trade-Related Aspects of Intellectual Property Rights, see The Sedona Conference, Framework for Analysis on Trade Secret Issues Across International Borders, 23 SEDONA CONF. J. 909 (2022).

³⁸ See, e.g., DTSA 18 U.S.C. § 1837 *v. Personalize Inc. v. Magnetize Consultants Ltd.*, 437 F. Supp. 3d 860, 878–79 (W.D. Wash. 2020) (stating that “18 U.S.C. § 1837 authorizes civil enforcement actions against foreign entities to the same extent as criminal actions” and collecting cases); *Motorola Sols.*, 436 F. Supp. 3d at 1165 (holding that Section 1836 may have extraterritorial reach subject to the restrictions in Section 1837; *AtriCure, Inc. v. Jian Meng*, 842 F. App'x 974, 983 (6th Cir. 2021) (holding the Ohio Uniform Trade Secrets Act applies extraterritorially against Chinese Defendants concerning conduct in China); *Miller UK Ltd. v. Caterpillar Inc.*, No. 10-CV-03770, 2017 WL 1196963, at *7 (N.D. Ill. Mar. 31, 2017) (concluding that the Illinois Trade Secrets Act (ITSA) does have extraterritorial effect because the ITSA specifically states that “a contractual or other duty to maintain secrecy or limit use of a trade secret shall not be deemed to be void or unenforceable solely for lack of durational or geographical limitation on the duty.”).

evidence for such claims prior to, during, and after exiting a due diligence or relationship involving sharing trade secrets with a foreign receiving party.

- j) Regarding points a and h above, the U.S. International Trade Commission offers a favorable environment for companies to pursue trade secret misappropriation claims against foreign respondents.

B. POTENTIAL SOLUTIONS WHEN ENDING DUE DILIGENCE OR A RELATIONSHIP

1. Perform Obligations in Contractual Tools

- a. **Up-to-date identification of disclosing party's trade secrets disclosed, modified or jointly developed**
 - i. Acknowledged by recipient
 - ii. Securely held in confidence by
 - 1. Recipient's counsel or in escrow and
 - 2. Disclosing party
- b. **Understanding of departures of recipient personnel who:**
 - i. Were authorized to access or use the trade secrets or
 - ii. Departed under circumstances otherwise warranting such notice
- c. **Memorialize what can be done with modified or jointly developed assets:**
 - iii. Jointly developed trade secrets
 - iv. Jointly developed technology that incorporates a trade secret(s) of one or both parties
- d. **Is there a Residuals clause?**

2. Update Physical Tools

- a. Final Audit
- b. Final Inspection

3. Update Technological Tools

- a. Forensics

VII. Appendices

- Clean Room elements
- Contractual clauses