UIC
REVIEW OF INTELLECTUAL PROPERTY LAW

AUTOMATED TRADE SECRET ASSET MANAGEMENT: SFP CLASSIFICATION, EONA PROOFS, BLOCKCHAINING, AND DTSA CIVIL SEIZURE ORDERS

R. MARK HALLIGAN

ABSTRACT

Trade secrets are some of the most valuable intellectual property assets in the world. Many companies owe substantial growth in their market value to their trade secret assets. Executives at those same companies see safeguarding trade secrets as more critical than protecting other intellectual property assets. While most companies recognize the importance of protecting their trade secret assets, most of those companies still struggle and sometimes fail to adequately manage and protect those nearly invaluable assets. However, this no longer has to be the case. There is an intellectual property revolution on the horizon called automated trade secret asset management ("TSAM"). Automated TSAM will allow companies to utilize the power of modern technology to effortlessly and efficiently identify, classify, protect, and value trade secret assets. The author has spent over 20 years developing an automated TSAM system. In this article, the author explores and explains the three critical building blocks necessary to create an automated TSAM: (1) Subject, Format, Product Classification (SFP Classification); (2) the Evidence, Ownership, Notice, and Access proof requirements (EONA Proofs); and (3) blockchain and hash codes. The author also explains how the automated TSAM will drastically reduce fruitless discovery and litigation costs and provide the trade secret holder with a more efficient path to utilizing Defend Trade Secret Act (DTSA) civil seizure orders.

UIC JOHN MARSHALL LAW SCHOOL

Cite as R. Mark Halligan, *Automated Trade Secret Asset Management: SFP Classification, EONA Proofs, Blockchaining, and DTSA Civil Seizure Orders*, 20 UIC REV. INTELL. PROP. L. 145 (2021).

AUTOMATED TRADE SECRET ASSET MANAGEMENT: SFP CLASSIFICATION, EONA PROOFS, BLOCKCHAINING, AND DTSA CIVIL SEIZURE ORDERS

R. MARK HALLIGAN

AUTOMATED TRADE SECRET ASSET MANAGEMENT: SFP CLASSIFICATION, EONA PROOFS, BLOCKCHAINING, AND DTSA CIVIL SEIZURE ORDERS

R. MARK HALLIGAN*

I. INTRODUCTION

Trade secrets are intangible intellectual property assets that impart substantial economic value because they provide a proprietary competitive advantage while excluding others from use. A massive percentage of any successful corporation's market value can be attributed to its intangible assets; often times, its trade secret information.[1] Therefore, if a company's trade secret information is such a large portion of its overall value, the loss or theft of that information can be catastrophic.[2] Thus, companies must be prepared. Companies must put in place an internal management system that pre-identifies and pre-classifies its trade secret assets before litigation ever ensues; this is where an Automated Trade Secrete Asset Management System becomes necessary.

Trade secret assets can be identified prior to litigation, but they must be validated in litigation.[3] This is compounded by the fact that there is no public registration system for trade secret assets; furthering the notion that companies or other enterprises must establish an *internal* trade secret asset management system.[4] As previously stated, an internal trade secret asset management system can ensure that a company is better prepared to identify and validate its trade secret assets if called into litigation.

The United States wields the most advanced legal system in the world for protecting trade secrets.[5] With state and federal statutory frameworks in place, trade secrets are defined broadly to include *any information* that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others.[6] This means that the modern

---

* © R. Mark Halligan. Mr. Halligan is a partner at FisherBroyles, LLP. Mr. Halligan focuses his practice on intellectual property litigation and complex commercial litigation, including trade secret, antitrust, and licensing issues. Chambers USA ranks Mr. Halligan as one of America's Leading Lawyers for Business in Intellectual Property law. The Legal 500 has inducted Mr. Halligan into the Legal 500 Hall of Fame for trade secret litigation. Mr. Halligan has served on the Adjunct Faculty of UIC John Marshall Law School teaching advanced trade secrets law for 26 years. Mr. Halligan earned the Corporate LiveWire Innovator of the Year award in 2018 for his contributions to the field of automated trade secret asset management.

[1] R. MARK HALLIGAN & RICHARD F. WEYAND, TRADE SECRET ASSET MANAGEMENT 2018: A GUIDE TO INFORMATION ASSET MANAGEMENT INCLUDING RICO AND BLOCKCHAIN 12–13 (Weyand Associates, Inc. 2018).

[2] *Id.* at 14.

[3] Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1018 (1984).

[4] *See* R. Mark Halligan, *Protecting U.S. Trade Secret Assets in the 21st Century*, ABA (Sept./Oct. 2013), https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2013-14/september-october-2013/protecting_us_trade_secret_assets_the_21st_century/ ("U.S. companies have a corporate and fiduciary responsibility to develop internal trade secret asset management systems to protect these corporate trade secret assets.").

[5] *Id.*

[6] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (AM. LAW. INST. 1995).

definition of a trade secret can encompass not just one piece of information, but thousands, tens of thousands, even millions of pieces of information for statutory trade secret protection.[7]

Is it feasible for companies and organizations to internally manage intellectual property assets that could comprise of millions of pieces of information? The naysayers say it cannot be done. [8] This group includes many intellectual property lawyers and in-house counsel.[9] The naysayers proclaim that any attempt to rein in all the potential and actual pieces of information that can qualify as a trade secret is a futile exercise. It is the crazy equivalent of attempting to "boil the ocean." So, for most companies and other businesses, trade secret asset management is a non-starter.

However, an internal trade secret asset management system does not have to be a non-starter. For one, it does not have to be a manual process. A trade secret asset management system can harness the efficient and highly advanced computer technology the world has to offer. There are two reasons for the rejection of computer software designed to identify, classify, protect, and value trade secret assets. First, critics posit that putting all the trade secrets in one location would create a huge security risk.[10] Second, if the company fails to enter a "trade secret" into the trade secret asset management (TSAM) system, the company will forfeit its rights in the trade secret asset.[11] Both perceptions are inaccurate.

The actual trade secret assets are not captured and placed in one computer directory or server farm. Instead, the automated TSAM system captures metadata about the trade secret asset. The term 'metadata" is data that describes and gives information about other data.[12] An old-school example is the card catalog that contains information about the contents of that library including the title of the book, the author of the book, the year of publication, the number of pages, the reference number in the Library of Congress, and the library call number (row and section) in the particular

---

[7] *Number of sent and received e-mails per day worldwide from 2017 to 2024*, STATISTA, https://www.statista.com/statistics/456500/daily-number-of-e-mails-worldwide/ (last visited Nov. 6, 2020) (Estimating that 306.4 billion emails will be sent and received each day in 2020 and this estimate is expected to increase to over 361.6 billion daily emails in 2021. So "millions" of pieces of confidential information in "daily" emails is a very infinitesimal amount).

[8] James Pooley, *No, You Don't Have to Inventory All Your Trade Secrets*, POOLEY (Feb. 28, 2016), https://www.pooley.com/single-post/2016/02/28/No-You-Dont-Have-To-Inventory-All-Your-Trade-Secrets.

[9] Beck Reed Riden, *A Primer and Checklist for Protecting Trade Secrets*, FAIR COMPETITION LAW (May 17, 2020), https://www.faircompetitionlaw.com/2020/05/17/a-primer-and-checklist-for-protecting-trade-secrets-and-other-legitimate-business-interests-before-during-and-after-lockdown-and-stay-at-home-orders/.

[10] *See* R. Mark Halligan, *The Next revolution in Intellectual Property Law: Automated Trade Secret Asset Management*, ABA (May/June 2019), https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2018-19/may-june/the-next-revolution-intellectual-property-law-automated-trade-secret-asset-management/ (An automated trade secret asset management system should capture only the metadata relating to trade assets. The TSAM system never exposes the actual trade secret. Instead it provides a pointer to the trade secret asset.).

[11] HALLIGAN & WEYAND, *supra* note 1 (A trade secret asset management (TSAM) system encompasses the identification, classification, protection and valuation of trade secret assets.).

[12] *What is Metadata Management*, INFORMATICA, https://www.informatica.com/resources/articles/what-is-metadata-management.html. (last visited Feb. 6, 2021).

library.[13] This is metadata: data [the card catalog] that provides information about other data [the book]. An automated TSAM system operates the same way: the system captures metadata relating to the trade secret; not the trade secret itself. The pointer to the "book" or "trade secret" exists independent of the actual contents of the "book" or "trade secret." An automated TSAM system reduces the risk of loss and allows metadata to be retrieved in seconds.[14]

Next, the determination whether a piece of information is a trade secret depends on proving the statutory requirements for a trade secret.[15] An automated TSAM system is merely a tool to assist companies with trade secret asset management. It is not meant to replace the state and federal statutory requirements for what information can be classified as a protectible trade secret. There is no legal requirement in the Uniform Trade Secrets Act (UTSA) or the Defend Trade Secrets Act (DTSA) that every trade secret be entered into some sort of trade secret asset management system.[16] The existence of metadata regarding a particular trade secret in the automated TSAM system merely serves as a concrete starting point to identify one's trade secrets and establish a viable cause of action for trade secret misappropriation. An automated TSAM system is lightning fast, making retrieval of critical information possible in

---

[13] *Trade Secret Examiner,* TRADE SECRET OFFICE, www.thetso.com/Software.html (last visited Oct. 27, 2020).

[14] *Id.*

[15] UNIFORM TRADE SECRETS ACT, 14 U.L.A § 1(4) [hereinafter UTSA]. The Uniform Trade Secrets provides the following definition for "trade secret":

> 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.

See also Defend Trade Secrets Act, 18 U.S.C. § 1839(3) [hereinafter DTSA]. The DTSA provides the following definition for "trade secret":

> the term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—
> (A)the owner thereof has taken reasonable measures to keep such information secret; and
> (B)the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.

[16] UTSA, *supra* note 15, § 1(4)(ii) (The [trade secret] is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.); *see also* DTSA, *supra* note 15, § 1839(3)(A) (The owner [of the trade secret] has taken reasonable measures to keep such information secret.).

seconds. If the piece of information qualifies as a trade secret under the UTSA or DTSA, it is a trade secret, regardless whether the metadata exists or not.[17]

The constant refrain that an automated TSAM system may "leave something out" and result in the forfeiture of trade secret rights is a cop-out. This is not a valid excuse for leaving trade secret assets in a state of chaos in most companies and organizations.[18] Boiler-plate NDA agreements are not a panacea. The law requires that reasonable measures be taken to protect trade secret assets.[19] The implementation of an automated TSAM system is a tool to assist the company in managing trade secret assets. If something is left out of the system, the confidential information will still qualify as a trade secret if it meets the statutory requirements for protection as a trade secret.[20]

Recent studies show that over eighty percent of senior executives recognize that trade secrets are critical and essential to their businesses.[21] Fifty percent of the senior executives say that trade secrets are more important than their patents and trademarks.[22] Even more (sixty-nine percent) say they foresee trade secret protection becoming more critical than safeguarding other types of intellectual property because of the rapid and furious pace of innovation.[23]

So why is there a disconnect between the recognition of the importance of trade secret assets and the failure of companies to manage the trade secret assets? Because, until recently, no one had a solution to this impending problem. This no longer has to be the case. The next revolution in intellectual property law will launch the implementation of automated TSAM systems designed to identify, classify, protect, and value trade secret assets.[24]

The author has spent over twenty years developing an automated trade secret asset management system. Along the way, there have been critical discoveries and watershed events that now underpin an automated trade secret asset management system. This article will explore the trial-and-error discovery of three critical building blocks used to create an automated TSAM system: SFP Classification, the EONA Proofs, and Blockchain and hash codes. Finally, the article will also address the absolute necessity of an automated trade secret asset management system for DTSA *ex parte* seizure orders.

---

[17] HALLIGAN & WEYAND, *supra* note 1

[18] Donal O'Connell & David Cohen, *Directors' Fiduciary Duty With Respect to Trade Secret Asset Management*, LINKEDIN (Nov. 2, 2018), https://www.linkedin.com/pulse/directors-fiduciary-duty-respect-trade-secret-asset-donal-o-connell/.

[19] UTSA, *supra* note 15, § 1(4)(ii) (The [trade secret] is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.); *see also* DTSA, *supra* note 15, § 1839(3)(A) (The owner [of the trade secret] has taken reasonable measures to keep such information secret.).

[20] Halligan, *supra* note 10, ch. 3.

[21] *The Board Ultimatum: Protect and Preserve*, BAKER MCKENZIE. https://www.bakermckenzie.com/-/media/files/insight/publications/2017/trade-secrets. (last visited Nov. 1, 2020).

[22] *Id.*

[23] *Id.*

[24] Halligan, *supra* note 10.

II. SUBJECT-FORMAT-PRODUCT (SFP) CLASSIFICATION

Taxonomy is the process of naming and classifying things. The starting point and ending point in trade secret law posits the following question: What is "IT" that is alleged to be the trade secret? The SFP System is a taxonomy that identifies and classifies trade secrets: [Subject] [Format] for [Product].[25] The *Subject* corresponds to the department or other organization that developed or uses the trade secret. Examples include research and development, manufacturing, quality control, and marketing. The *Format* identifies the receptacle for the trade secret: a formula, drawing, process, pattern, device, method, techniques, designs, plans, programs, codes, and the like. The *Product* identifies an existing product, a prototype, or a failed product.

Here are several examples:

> Engineering Specifications for the Model 5750 tractor. [Engineering] is the Subject. [Specifications] is the Format. Model 5750 Tractor is the [Product].
>
> Sales Plan for Lawn Furniture. [Sales] is the Subject. [Plan] is the Format. Lawn Furniture is the [Product].
>
> Manufacturing Drawings for Sootblower. [Manufacturing] is the Subject. [Drawing] is the Format. Sootblower is the [Product].
>
> Research Test Results for Non-Flammable Plastics. [Research] is the [Subject]. [Test Results] is the Format. Non-Flammable Plastics is the [Product].

The SFP classification system enables granular categorization of a larger universe of trade secret assets. At first blush, it seems too rudimentary for complex pieces of information within an organization. Just the opposite is true. The SFP classification system pinpoints the existence of a trade secret within a three-dimensional plane. Each trade secret lies within one SFP cubby-hole**.**

[25] *Id*. ch. 12.

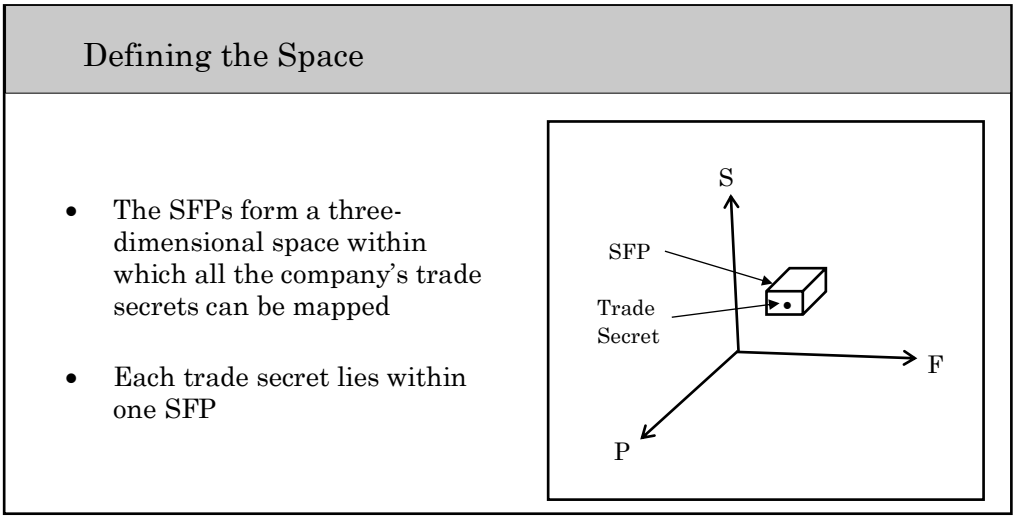

Figure 1

Let's take an example of a company with 10 departments, 30 formats for proprietary information, and 20 products. This company has 6,000 SFP cubby-holes available into which tens of thousands or even millions of trade secrets can now be efficiently sorted.

Classification by SFP is well suited for computerized trade secret asset management because once all the possible Subjects, Formats, and Products have been identified, assigning any particular piece of information to an SFP cubby-hole is simply a matter of selecting the appropriate **S**, **F,** or **P** from three drop-down boxes custom-built into the SFP database. Another benefit is the ability to sort the SFP cubby-holes by Subject, by Format, and by Product.

The SFP classification system is simple for employees to use. Employees are already knowledgeable about the different departments within the company, the different types of information, and the different products that the company manufactures and sells. Little to no employee training is required to use these 6,000 SFP cubby-holes since employees know what constitutes an [Advertising[[Plan] for [Snack Products] or [Packaging] [Design] for [Laundry Detergent].

III. EXISTENCE-OWNERSHIP-NOTICE-ACCESS (EONA) PROOFS

Legal recognition of a piece of information as a trade secret requires litigation and proof by a preponderance of evidence that the piece of information satisfies the statutory criteria outlined in the UTSA or DTSA.

Until the trial court grants the trade secret owner's motion for summary judgment that "X" is a trade secret or until the judge or jury returns a verdict that "X" is a trade secret, the piece of information remains as just an alleged trade secret. Alternatively,

the judge or the jury could also determine that the information at issue is not a trade secret, preventing the plaintiff from unilaterally classifying it as such in the future.

A plaintiff must submit evidentiary proof of existence, ownership, notice, and access in order to adequately prove that the information at issue is a protectible trade secret. These proofs – existence, ownership, notice, and access – are called the "EONA" proofs and are unique to trade secret law.[26] If a plaintiff adequately proves each of the four EONA proofs, odds are that the judge or the jury will return a finding that the information at issue is a trade secret under either the UTSA or DTSA.

Each of the EONA Proofs are reviewed below.

A. *Existence Proofs*

The existence of a "trade secret" is one of the most elusive and difficult concepts in the law to define.[27] There is no exact definition of a trade secret due to the vast spectrum of information that could qualify as such. Additionally, the wide array of factual circumstances that could be determinative or fatal to a piece of information's possible classification as a trade secret contributes to the malleable definition of a trade secret.

The question whether an alleged piece of information qualifies as a trade secret is a question of fact to be determined by the trier of fact upon the greater weight of the evidence.

The statutory provisions defining a "trade secret" in the UTSA and DTSA focus on the secrecy and value of the information as well as the reasonable efforts by the trade secret owner to maintain secrecy and confidentiality.[28]

However, these statutory requirements are not evidentiary, and they do not flush out the fact-intensive factors to be considered in ascertaining whether a trade secret exists.

The key litmus test in trade secrets law is the **six-factor test** identified by the American Law Institute in 1939 after a review of over 100 years of case law in the 19th Century.[29] Today, the six-factor test has been adopted by virtually every state and federal court in the United States.[30] The attraction of the six-factor test is its ability to evaluate any type of potential trade secret under any set of factual circumstances. It is extraordinarily versatile and compatible with modern statutory trade secret law.

The six-factor test is miraculous in its predictive capabilities. The six-factor test evaluates the "strength" of the alleged trade secret: ranging from strong trade secret,

---

[26] Halligan, *supra* note 10.

[27] Learning Curve Toys, Inc. v. PlayWood Toys, Inc., 342 F.3d 714, 723 (7th Cir. 2003); Lear Siegler, Inc. v. Ark–Ell Springs, Inc., 569 F.2d 286, 288 (5th Cir. 1978).

[28] *Learning Curve Toys, Inc.*, 342 F.3d at 721 (The Act's statutory requirements focus fundamentally on the secrecy of the information sought to be protected.). *See* UTSA, *supra* note 15, § 1(4)(ii) (stating that trade secrets must be "subject of efforts that are reasonable . . . to maintain its secrecy"); DTSA, *supra* note 15, § 1839(3)(A) (stating that the trade secret owner "has taken reasonable measures to keep [the] information secret").

[29] RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (AM. LAW. INST. 1939).

[30] *See Learning Curve Toys*, 342 F.3d at 714; *In re* Bass, 113 S.W.3d 735, 739 (Tex. 2003); State ex rel. Plain Dealer v. Ohio Dept. of Insurance, 80 Ohio St. 3d 513, 525 (1997). *See* Appendix A for additional cases illustrating various courts' adoption and utilization of the six-part test for trade secret viability from the RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (AM. LAW. INST. 1939).

to weak trade secret, to no trade secret. All six factors must be considered first, one-by-one, and then together as a whole.

The six factors are set forth below with the rationale for each factor in parentheses:[31]

> Factor 1: The extent to which information is known outside the company (the more extensively the information is known outside the company, the less likely that it is a protectable trade secret).
>
> Factor 2: The extent to which the information is known by employees and others involved in the company (the greater the number of employees who know the information, the less likely that it is a protectable trade secret).
>
> Factor 3: The extent of measures taken by the company to guard the secrecy of the information (the greater the security measures, the more likely that it is a protectable trade secret).
>
> Factor 4: The value of the information to the company and competitors (the greater the value of the information to the company and its competitors, the more likely that it is a protectable trade secret).
>
> Factor 5: The amount of time, effort and money expended by the company in developing the information (the more time, effort and money expended in developing the information, the more likely that it is a protectable trade secret).
>
> Factor 6: The ease or difficulty with which the information could be properly acquired or duplicated by others (the easier it is to duplicate the information, the less likely that it is a protectable trade secret).

The six-factor test is well suited for automated trade secret asset management. Each alleged trade secret can be scored on each of the six factors using a one-to-five scale. Everyone is familiar with one-to-five scoring from product rankings to the ubiquitous A-B-C-D-F grading system. This creates a composite mathematical score for each alleged trade secret which allows the trade secret owner to identify and classify trade secret assets. The higher scores mean stronger trade secrets; lower scores mean weaker trade secrets.

Using an automated TSAM system, the trade secret holder can now evaluate and rank trade secret assets *before* any potential trade secret litigation providing the litigation team with strategic options to choose the battleground.

---

[31] RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (AM. LAW. INST. 1939).

B. *Ownership Proofs*

The "ownership" proof requires the holder of the trade secret to prove ownership.[32] The existence of a trade secret precedes ownership of a trade secret. If a piece of information is generally known in the trade, or if it is readily ascertainable by proper means, then ownership becomes irrelevant because anyone can disclose or use the piece of information. The world "owns" it.

There is no definition of "owner" in the UTSA. However, the DTSA defines the term "owner" as "the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed."[33] Therefore, there can be multiple "owners" of a trade secret.

One context in which trade secret ownership is often disputed is in the employment context. Employers and employees often quarrel as to who is the rightful owner of a particular trade secret. An added wrinkle in this context is that there is no "work for hire" doctrine in trade secrets law. Absent a contrary agreement, the law assigns ownership in an invention or idea to the person who conceives it.[34] Similar to other employment and ownership contexts, agency law guides and determines the allocation of ownership between employers and employees.[35] Additionally, employees retain ownership of information comprising their general knowledge, skills, and experience.[36] However, there is a narrow exception to the general rule called the "hired to invent" doctrine: If an employer hires you to do experimental work for inventive purposes then the employer owns the fruit of you labor under the "hired to invent" doctrine.[37]

There are three illustrations of "ownership" of trade secrets in the Restatement (Third) of Unfair Competition:[38]

> (1) A, a manufacturer of household chemicals, employs B, a chemist to develop new products. In the course of the employment, B develops a formula for a new floor cleaner that is a significant improvement over

---

[32] MAI Sys. Corp. v. Peak Comput., Inc., 991 F.2d 511, 522 (9th Cir. 1993) (to prove ownership of a trade secret, plaintiffs "must identify the trade secrets and carry the burden of showing they exist") (citing Diodes, Inc. v. Franzen, 260 Cal. App. 2d 244, 249 (Cal. Ct. App. 1968)); *see also* Inteliclear, LLC v. ETC Glob. Holdings, Inc., 978 F.3d 653, 658 (9th Cir. 2020); CytoDyn of New Mexico Inc. v. Amerimmune Pharmaceuticals, Inc. 160 Cal. App. 4th 288, 297 (Cal. Ct. App. 2008); Space Data Corp. v. X, No. 16-cv-03260 BLF, 2017 WL 5013363, at *2 (N.D. Cal. Feb. 16, 2017) (ownership is an essential element for trade secret protection. To plead a trade secret claim, the plaintiff must first establish that it owned a trade secret. To do so, the plaintiff must describe the alleged trade secret "with sufficient particularity to separate it from matters of general knowledge") (quoting Pellerin v. Honeywell Int'l, Inc., 877 F. Supp. 2d 983, 988 (S.D. Cal. 2012); Nickelson v. General Motors Corp., 361 F.2d 196, 198 (7th Cir. 1966) (the plaintiff must prove the existence and ownership of a trade secret).

[33] DTSA, *supra* note 15, § 1839(4).

[34] United States v. Dubilier Condenser Corp., 289 U.S. 178, 187 (1933).

[35] RESTATEMENT (SECOND) OF AGENCY § 397 (AM. LAW. INST. 1958).

[36] *See, e.g.*, Valco Cincinnati, Inc. v. N & D Machining Serv., Inc., 24 Ohio St. 3d 41, 47 (Ohio 1986).

[37] Solomons v. United States, 137 U.S. 342, 346 (1890); Computer Assocs. Int'l. v. American Fundware, 831 F. Supp. 1516, 1524 (D. Colo. 1993); Vigitron, Inc. v. Ferguson, 120 N.H. 626, 628 (N.H. 1980).

[38] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 42 cmt. e, illus. 1–3 (AM. LAW. INST. 1995).

existing product. After leaving the employment with A, B is induced by C, a competitor of A, to disclose the secret formula. Because B was hired by A specifically to develop new products, the formula is owned by A; B and C are now subject to liability to A.

(2) The facts as being otherwise as stated in Illustration 1, B is hired by A to analyze the formulas of products sold by A's competitors. After leaving the employment with A, B is hired to perform a similar task for C, a competitor of A. In analyzing the formulas for C, B relies on the general skill and training acquired during the former employment. B and C are not subject to liability to A.

(3) A is a toy maker. B, who is hired by A as a toy designer, invents a new manufacturing process that is valuable to A's business. B terminates the employment with A and begins work for C, a competing toy maker, and assists in implementing the new manufacturing process at C's factory. Because the new process was not the product of B's assigned duties while employed by A, in the absence of an agreement to the contrary, the rights in the process are owned by B; B and C are not subject to liability to A. However, A may have a "shop right" in the manufacturing process if B developed the process using A's time, personnel, facilities or equipment.[39]

The first illustration is an application of the "hired to invent" doctrine.[40] The second illustration is an example of the rule that an employee retains ownership of his general skill and training. The third illustration applies the common law rule that the employee owns the invention, but the employer retains a "shop right" in the manufacturing process—an irrevocable, nonexclusive, royalty-free license—because the manufacturing process was developed using the employer's time, personnel, facilities and equipment.[41]

Proving ownership of a trade secret is not an easy task. If the evidence establishes that A is the owner of the trade secret, then A has standing to file a complaint for trade secret misappropriation. If B is the owner of the trade secret, then A does not have standing to sue B for trade secret misappropriation. Additionally, if an employee develops a new trade secret at their company, but then leaves that company, that employee owns the trade secret absent a successful application of the hired to invent doctrine, which would transfer ownership to the employer after the employee's departure. However, if the former employee used the former employer's personnel,

---

[39] *Dubilier Condenser Corp.*, 289 U.S. at 178 ("inventions of a general employee belong to the employee, but if the employee uses the employer's time, materials, and facilities in developing the invention, the employer is entitled to a nonexclusive, irrevocable license.").

[40] *See* Farmers Edge, Inc. v. Farmobile, LLC, 970 F.3d 1027, 1032 (8th Cir. 2020) (explaining the hired-to-invent doctrine as "[w]hen an employee is hired to devote his efforts to a particular problem, to conduct experiments for a specifically assigned purpose, and an invention results from the results of that work, it belongs to the employer.").

[41] *Dubilier Condenser Corp.*, 289 U.S. at 178 ("inventions of a general employee belong to the employee, but if the employee uses the employer's time, materials, and facilities in developing the invention, the employer is entitled to a nonexclusive, irrevocable license.").

facilities or equipment to create the trade secret, then the former employer has a "shop right" to practice the trade secret and the former employee cannot sue the former employer for trade secret misappropriation.

Another complicated issue in trade secret ownership is that there exists the possibility of lawful concurrent ownership and usage of a similar or the same trade secret absent a license. For example, if a third party acquires a trade secret by lawful means, such as reverse engineering or independent development, then the third party becomes an "owner" of the trade secret. They then cannot be sued for trade secret misappropriation and have full ownership interest in their discovery.

These rules of "trade secret" ownership can be altered by contract. The execution of a valid and enforceable assignment can transfer ownership of an invention or trade secret from the employee to the employer.[42] To obtain ownership of a trade secret belonging to an employee, the employer must execute a valid and enforceable assignment transferring ownership of the trade secret from the employee to the employer.[43]

C. *Notice Proofs*

The trade secret owner must show that the alleged misappropriator had actual, constructive, or implied notice of the alleged trade secret.[44] Notice requires identification of the alleged trade secret with particularity. An alleged trade secret must be described with sufficient specificity so that when a description of what is generally known in the industry is placed side-by-side with the description of the alleged trade secret, an adequate comparison can be made.[45]

---

[42] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 42 cmt. g (AM. LAW. INST. 1995).

[43] *See* Pullman Grp. V. Prudential Ins. Co. of Am., 288 A.D.2d 2, 3 (N.Y. App. Div. 2001). The court explains that there must be a valid and express assignment of a trade secret from the employee to the employer:

> Nor does plaintiff have standing by assignment, since the written assignments of rights and obligations in specified contracts from Gruntal to Fahnestock and, subsequently, from Fahnestock to plaintiff, make no mention of trade secrets or other intellectual property, and intent to assign a trade secret will not be imputed absent express, volitional conduct by the presumed assignor and assignee given that an assignment of a trade secret will permanently deprive the assignor of the use thereof (internal citation omitted).

[44] *See* Wyeth v. Natural Biologies, Inc., 395 F.3d 897, 900 (8th Cir. 2005). The court explains that the acquirer of a trade secret must have notice as to its trade secret status:

> The existence of a trade secret is not negated merely because an employee or other person has acquired the trade secret without express or specific notice that it is a trade secret if, under all the circumstances, the employee or other person knows or has reason to know that the owner intends or expects the secrecy of the type of information comprising the trade secret to be maintained.

(quoting Minn. Stat. § 325C.01, subd. 5).

[45] IDX Systems Corp. v. Epic Sys. Corp., 165 F. Supp. 2d 812, 816 (W.D. Wis. 2001).

The requirement of notice is a reasonable measure required to protect the secrecy of the piece of information alleged to qualify as a trade secret. It is improper to claim the existence of a trade secret after-the-fact.[46] To maintain the secrecy of a putative trade secret, the employer must place the employee on notice of the trade secret status of matters the employee is working on. The traditional means for placing an employee "on notice" is to require the employee to sign a secrecy agreement or a non-disclosure agreement.[47] When the time comes, notice can be proved by direct or circumstantial evidence. The Restatement (Second) of Torts provides an effective and useful foundation for defining what constitutes notice in the trade secret context, stating:

> One has notice of the facts when he knows of them or when he should know of them. He should know of them if, from the information which he has, a reasonable man would infer the facts in question, or if, under the circumstances, a reasonable man would-be put-on inquiry and an inquiry pursued with reasonable intelligence and diligence would disclose the facts.[48]

The "notice" requirement in trade secrets law is the linchpin for imposing liability on the alleged trade secret misappropriator. There is no liability if there is no notice of the confidential character of the disclosure. If A discloses the secret to B despite B's protest that he does not wish to hold the secret in confidence and will not so hold it if it is disclosed, there is no breach of confidence and no liability.[49]

It is a fundamental tenet of trade secret law that an unprotected disclosure of confidential information to the receiving party vitiates the status of the information as a trade secret. It is like a "pin pricking a balloon"—the status of the information as a protectable trade secret asset is forfeited as a matter of law.[50]

D. *Access Proofs*

It is vital for a trade secret misappropriation claim that the existence of a trade secret be proven.[51] But it is also necessary that the plaintiff allege and prove that the

---

[46] *See* UTSA, *supra* note 15, § 4; DTSA, *supra* note 15, § 1836(b)(3)(D) (Under the UTSA and DTSA, if a claim of trade secret misappropriation is made in bad faith, reasonable attorney's fees may be awarded. The DTSA also adds the language that bad faith may be established by circumstantial evidence.).

[47] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 41 (AM. LAW. INST. 1995) ("A duty of confidence can be created by an express promise of confidentiality made by the recipient of the disclosure. A duty of confidence may also be inferred from the relationship between the parties and the circumstances surrounding the disclosure.").

[48] RESTATEMENT (SECOND) TORTS § 757 cmt. l (AM. LAW. INST. 1939).

[49] *Id.* § 757 cmt. j.

[50] Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 490 (1974).

[51] Zemco Manufacturing, Inc. v. Navistar International Transportation Corp., 759 N.E.2d 239, 253 (Ind. Ct. App. 2001) ("If there is no trade secret, there can be no misappropriation."); Goodbye Vanilla, LLC v. Aimia Proprietary Loyalty U.S., Inc., 304 F. Supp. 3d 815, 820 (D. Minn. 2018) ("Without a proven trade secret there can be no action for misappropriation") (quoting Electro-Craft Corp. v. Controlled Motion, Inc., 332 N.W.2d 890, 897 (Minn. 1983)).

defendant had access to, and further, improperly acquired the alleged trade secret.[52] Once the existence of a trade secret and defendant's access or improper acquisition of that trade secret is proven, the trade secret misappropriation claim can proceed.

Assuming the existence of at least one trade secret, there are three forms of misappropriation under the UTSA and DTSA: unauthorized acquisition, unauthorized disclosure, and unauthorized use.[53] This all stems from the defendant's access to the alleged trade secret.

There must be proof of "access." This is a typical fact pattern:

1. An employee acquires Trade Secret A from the existing employer;
2. The employee resigns and joins a competitor (new employer);
3. The former employee takes Trade Secret A with him to the new employer;
4. The former employee discloses Trade Secret A to the new employer;
5. The new employer and the former employee use Trade Secret A.

The entire fact pattern is triggered by the initial acquisition of Trade Secret A by the employee. Without access and acquisition, there can be no liability for trade secret misappropriation. Acquisition of a trade secret by improper means is wrongful.[54]

---

[52] Zellweger Analytics, Inc. v. Milgram, No. 95 C 5998, 1997 U.S. Dist. LEXIS 16539, at *9 (N.D. Ill 1997) (Summary judgment for defendants granted; the record showed that plaintiff failed to discover any evidence proving that the new employer used or relied on the two alleged trade secrets.).

[53] UTSA, *supra* note 15, § 1(2); DTSA, *supra* note 15, § 1839(5). The statutory definition of misappropriation in the UTSA and DTSA:

> (1) "Improper means" shall include theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means.
> (2) "Misappropriation" shall mean:
> a. Acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or
> b. Disclosure or use of a trade secret of another without express or implied consent by a person who:
> 1. Used improper means to acquire knowledge of the trade secret; or
> 2. At the time of disclosure or use, knew or had reason to know that his or her knowledge of the trade was:
> A. Derived from or through a person who had utilized improper means to acquire it;
> B. Acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or
> C. Derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or
> 3. Before a material change of the person's position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.

[54] Anheuser-Busch Cos. v. Clark, No. 2:13-cv-00415-TLN-CKD, 2017 U.S. Dist. LEXIS 42680, at *9 (E.D. Cal. Mar. 23, 2017). The court states the UTSA's definition for trade secret misappropriation:

> A claim for misappropriation of trade secrets under UTSA requires the plaintiff to demonstrate the defendant acquired, disclosed, or used the plaintiff's trade secret through improper means. UTSA defines 'misappropriation' as an '[a]cquisition of a trade secret of another by a person who knows or has reason to know that the trade

Acquisition of a trade secret by proper means is lawful.[55] Whether by "proper" means or "improper" means there must be proof of the defendant's "access" to the trade secret. Otherwise, the trade secret owner cannot establish a *prima facie* cause of action for trade secret misappropriation. Unlike the holder of a patent, the owner of a trade secret has no claim against another who independently discovers or reverse engineers the trade secret.[56] Therefore, it is crucial that a plaintiff adequately prove that the defendant had access to and improperly acquired the alleged trade secret.

The EONA proofs serve as a guide; a framework for what a trade secret owner must know and be ready to prove regarding their proprietary trade secret information. First, a trade secret owner must demonstrate that what they claim is a trade secret, is in fact a trade secret. The definitions in the UTSA and DTSA, along with the Restatement's six-factor litmus test, provide more than adequate guideposts to allow trade secret owners to evaluate the validity and potential existence of their trade secret information. Second, a trade secret owner must show that they actually are the rightful owner of the alleged trade secret information. Third, a trade secret owner must show that they provided adequate notice to internal employees and the outside world that the alleged trade secret is proprietary and confidential. And finally, a trade secret owner must be able to prove that the alleged misappropriator had access to its trade secret prior to the alleged misappropriation. These aforementioned proofs will ensure that a trade secret owner is prepared to litigate its trade secret. An automated TSAM system captures and monitors information relevant to these proofs, further streamlining the ability of the trade secret owner to internally protect its trade secret information.

IV. BLOCKCHAINS AND HASH CODES

The rules of evidence require authentication of the evidence.[57] The proponent must produce evidence to support a finding that the item of evidence is what the proponent claims it is.[58] Trade secret disputes are fact intensive. The EONA proofs require proof of existence, ownership, notice, and access for each alleged trade secret by a preponderance of the evidence. Issues relating to whether a piece of information is generally known in the trade presents questions of fact. Issues relating to whether a piece of information is readily ascertainable by proper means presents questions of fact. Issues relating to whether there was acquisition of the trade secret by proper or

> secret was acquired by improper means.' 'Improper means' includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means. (internal citations omitted).

[55] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 cmt. b (AM. LAW. INST. 1995) ("Unless a trade secret has been acquired under circumstances giving rise to a duty of confidence, a person who obtains the trade secret by proper means is free to use or disclose the information without liability.").

[56] *Kewanee Oil Co.*, 416 U.S. at 470.

[57] Fed. R. Evid. 901(a); I.R.E. 902(12)–(13); Illinois Blockchain Technology Act, 205 ILL. COMP. STAT. 730.

[58] Fed. R. Evid. 901(a); I.R.E. 902(12)–(13); Illinois Blockchain Technology Act, 205 ILL. COMP. STAT. 730. *See also* Fed. R. Evid. 901(b)(9) (This section of the authentication rule allows for authentication of "a process or system" with evidence "describing [the] process and showing that it produces an accurate result.").

improper means presents questions of fact. Issues relating to whether reasonable measures have been taken to maintain the secrecy of the alleged trade secret present questions of fact. All in all, trade secret identification and misappropriation present fact intensive inquiries.

It seems overwhelming. Litigation fees in trade secret disputes are skyrocketing. However, there is a solution. Many factual disputes can now be eliminated by using an automated TSAM system with blockchain. In short, blockchain is a digital open ledger system that records and tracks information on a peer-to-peer network.[59] All new information that is added to the blockchain must be verified and is then time stamped, creating an immutable transaction history and chain of custody. This means that blockchain evidence is self-authenticating and tamper-free evidence. Using the blockchain, the proof that the item of evidence is what the proponent claims it is cannot be refuted.

To understand blockchains, one must first understand hash codes.[60] A computer hash code is a string of characters that can be generated by a computer from any digital input. It is a one-way cryptographic function that accepts a message of any length as input and returns as output a fixed-length digest value to be used for authentication of the original message. It is a mathematical process that is repeatable and one-way only: the same input will always generate the same hash code. A hash code is not an encryption algorithm. It is not reversible, and it cannot be decrypted back to the original input.

Digital forensic experts use hashing methods to verify that *copies* of digital evidence match the *original data* from which the copies are made, i.e. the hashes or "fingerprints" match. The SHA-256 hashing algorithm produces a 256-bit hash value and a 64-character alphanumeric fingerprint. Here is an example of "hash-coding" for the datum – trade secret – to binary context:

55594b7c3bc5022928d827895c55a6b5bc0391991cb25b8c3e52d5bc0411c3b7

Each digit is one of sixteen values, from 0-9 and A-F, each of which represents 4 bits (0000, 0001, 0010, 0100). The 64-character hash code has 256 bits. A 256-bit hash has so many possibilities that you could give a unique serial number to every neutron, proton, and electron in the Milky Way galaxy, a million times over, and still use only half of the possible alphanumeric fingerprints.[61]

---

[59] *See* George Bellas, *Blockchain as Evidence*, ISBA (Nov. 2019), https://www.isba.org/sites/default/files/sections/civilpracticeandprocedure/newsletter/Civil%20Practice%20and%20Procedure%20November%202019.pdf. *See* Illinois Blockchain Technology Act, 205 ILL. COMP. STAT. 730/1.

[60] *The Sedona Conference Glossary: E-Discovery and Digital Information Management (4th Edition)*, 15 SEDONA CONF. J. 305, 330 (2014), https://thesedonaconference.org/sites/default/files/publications/The%20Sedona%20Conference%20Glossary%204d%20Journal%202014.pdf (the "hash code" of a record is defined as "a mathmatical algorithm that calculates a unique value for a given set of data, similar to a digital fingerprint, representing the binary content of the data to assist in subsequently assuring that data has not been modified").

[61] *See SHA-256 Cryptographic Hash Algorithm*, MOVABLE TYPE SCRIPTS, https://www.movable-type.co.uk/scripts/sha256.html (last visited November 1, 2020).

A blockchain is a set of entries in "blocks," each of which is mathematically linked to the one before it by hash codes.[62] For instance, an example of an entry in the blockchain is as follows:

Data n, timestamp n, hashcode (hashcode n-1, data n, timestamp n).

The next entry in the blockchain contains the new data, the current timestamp, and a hash code created from the last entry's hashcode data and timestamp. This is the beauty of blockchaining. It creates a comprehensive and immutable time stamped transaction history for all of the information on the blockchain, creating evidence that is self-authenticating.

The automated TSAM system links hash codes in blocks without the necessity of using a third-party time-stamping authority. Using hash codes and blockchain technologies in an automated TSAM system is a game changer. Once trade secret metadata is entered into the blockchain, there is no possibility of records being altered or falsified. You cannot go backward in the blockchain—blocks only go forward. Proof of the existence of a trade secret, ownership, notice, and access can now be instantly proved by production of the timestamped blockchain digital records on any date of interest in a trade secret misappropriation lawsuit.

V. AUTOMATED TRADE SECRET ASSET MANAGEMENT AND DTSA CIVIL SEIZURE ORDERS

In 2008, the author wrote a law review article for the UIC Review of Intellectual Property Law (formerly the John Marshall Review of Intellectual Property Law) recommending two critical amendments to the Economic Espionage Act of 1996—a private civil cause of action and a statutory provision for issuing *ex parte* seizure orders.[63] Eight years later in 2016, both these recommendations were enacted into law in the Defend Trade Secrets Act of 2016.[64]

The DTSA is a watershed event in intellectual property law. The Senate passed the DTSA on April 4, 2016 (87-0).[65] The House of Representatives passed the DTSA on April 27, 2016 (410-2).[66] President Obama signed the DTSA into law on May 11, 2016.[67]

Trade secret assets are now on the same playing field as patents, copyrights, and trademarks. The DTSA creates a private civil cause of action for trade secret misappropriation.[68] Powerful trade secret protection tools are built into the DTSA including the addition of *ex parte* seizure provisions.

---

[62] *See* Illinois Blockchain Technology Act, 205 ILL. COMP. STAT. 730/5 (A blockchain "means an electronic record created by the use of a decentralized method by multiple parties to verify and store a digial record of transactions which is secured by the use of a cryptographic hash of previous transaction information").

[63] R. Mark Halligan, *Protection of U.S. Trade Secret Assets: Critical Amendments to the Economic Espionage Act of 1996*, 7 J. MARSHALL REV. INTELL. PROP. L. 656 (2008).

[64] DTSA, *supra* note 15, § 1836(b)(1)–(2).

[65] *Defend Trade Secrets Act of 2016*, CONGRESS.GOV (July 29, 2015), https://www.congress.gov/bill/114th-congress/senate-bill/1890/text.

[66] *Id*.

[67] *Id*.

[68] DTSA, *supra* note 15, § 1836(b)(1).

Protecting trade secret assets requires the element of surprise. Today, a trade secret asset can be transferred anywhere in the world in a matter of seconds. Trade secret assets can also be destroyed in a matter of seconds.

A private civil cause of action, without more, is toothless. Without an *ex parte* order executed by surprise to secure the trade secrets and to prevent the destruction of evidence—the trade secret assets are in danger of being destroyed or transferred to bad actors around the world.

This is where the rubber meets the road. The trade secret victim must be prepared ahead of time to provide the evidence necessary to comply with the stringent DTSA requirements for an *ex parte* seizure order. The first step in the *ex parte* seizure process is filing a verified complaint or separate affidavit.[69] The trial court must find that "it clearly appears from specific facts" in the *ex parte* seizure application that the following eight enumerated requirements have been met:

(1) Other equitable relief, including injunctive relief under Rule 65 of the Federal Rules of Civil Procedure, is inadequate;

(2) Seizure is necessary to prevent an immediate and irreparable injury;

(3) The balancing of harms justifies the seizure;

(4) The applicant likely will succeed in showing the trade secret and the subject of the order misappropriated the trade secret by improper means or conspired to use improper means;

(5) The subject of the order has "actual possession" of the trade secret and any property;

(6) The matters to be seized are described "with reasonable particularity" and the location is identified "to the extent reasonable under the circumstances;

(7) The subject of the order "would destroy, move, hide, or otherwise make such matter inaccessible by the court" if notice were provided;

(8) The applicant has not publicized the request for seizure.[70]

These eight requirements assume that the trade secret owner has in place a sophisticated internal trade secret asset management system that can output the evidence in real time for emergency injunctive relief and issuance of an *ex parte* seizure order. The evidence of a trade secret must exist ahead of time; the trade secret owner must identify the trade secrets with reasonable particularity ahead of time; the matter to be seized and the location where the matter is to be seized needs to be identified ahead of time; the evidence of improper means must exist ahead of time; the detailed

---

[69] *Id.* § 1836(b)(2)(A)(i) (The application for a civil seizure order must be made by "affidavit or verified complaint" and present "specific facts" to support the findings of fact and conclusions of law entered by the court.).

[70] *Id.* § 1836(b)(2)(A)(ii).

description of the trade secrets to assist law enforcement during the seizure must exist ahead of time. A TSAM system ensures that a trade secret holder will have all of the aforementioned captured ahead of time; giving them a leg up on the misappropriator.

What does this mean for a company without an internal trade secret asset management system? It means that the company will have an incredibly difficult and inefficient path towards utilizing the powerful *ex parte* seizure provisions in the DTSA to protect corporate trade secret assets. What does this mean for companies with non-computerized trade secret asset management systems? It means that the misappropriator will have a huge advantage over the trade secret owner who cannot move as fast as the misappropriator. The outcome will be likely the same—no *ex parte* seizure order.

Implementing an automated TSAM system changes everything. It will enable companies to instantly and efficiently recall and generate the necessary information to satisfy the eight requirements for obtaining an *ex parte* seizure order. The automated TSAM system will not only enable companies to accurately and efficiently manage and organize its trade secrets assets, but also take full advantage of the legal enforcement mechanisms to protect their trade secrets from misappropriation.

VI. CONCLUSION

Trade secret owners must utilize modern technology in order to adequately and successfully identify, manage, and protect their trade secret assets; an automated trade secret asset management system is necessary. One automated trade secret asset management system, called The Trade Secret Examiner®, implements the software tools discussed in this article including SFP Classification, the EONA Proofs, and Blockchain and hash codes.[71] The DTSA provides U.S. companies with powerful tools to protect trade secret assets but companies cannot fully take advantage of these tools without the deployment of an automated TSAM system. Manual approaches to trade secret identification, classification, protection and valuation are too slow and archaic. Time is of the essence in a trade secret misappropriation lawsuit. The key to success under the DTSA requires the implementation of an automated trade secret asset management system.

[71] THE TRADE SECRET OFFICE, www.thetso.com (last visited Feb. 6, 2021).

APPENDIX A: ADDITIONAL CASES DEMONSTRATING THE ADOPTION AND UTILIZATION OF THE SIX-FACTOR TEST FOR TRADE SECRET VIABILITY FROM THE RESTATEMENT (FIRST) OF TORTS § 757 CMT. B (AM. LAW INST. 1939)

See Powercorp Alaska, LLC v. Alaska Energy Auth., 290 P.3d 1173 (Alaska 2013); Enterprise Leasing Co. of Phoenix v. Ehmke, 197 Ariz. 144 (Ariz. Ct. App. 1999); Bradshaw v. Alpha Packaging, Inc., 379 S.W.3d 536 (Ark. Ct. App. 2010); Se. X-Ray, Inc. v. Spears, 929 F. Supp. 2d 867 (W.D. Ark. 2013); Freeman v. Brown Hiller, Inc., 102 Ark. App. 76 (Ark. Ct. App. 2008); Wal-Mart Stores, Inc. v. the P.O. Mkt., Inc., 347 Ark. 651 (Ark. 2002); Tyson Foods, Inc. v. Conagra, Inc., 349 Ark. 469 (Ark. 2002); Weigh Systems South v. Mark's Scales Equipment, 347 Ark. 868 (Ark. 2002); Freeman v. Brown Hiller, Inc., 102 Ark. App. 76 (Ark. Ct. App. 2008); Wal-Mart Stores, Inc. v. the P.O. Mkt., Inc., 347 Ark. 651 (Ark. 2002); Weigh Systems South v. Mark's Scales Equipment, 347 Ark. 868 (Ark. 2002); City Slickers v. Douglas, 73 Ark. App. 64 (Ark. Ct. App. 2001); Conagra, Inc. v. Tyson Foods, Inc., 342 Ark. 672 (Ark. 2000); Walshe v. Zabors, 178 F. Supp. 3d 1071 (D. Colo. 2016); Electrology Lab., Inc. v. Kunze, 169 F. Supp. 3d 1119 (D. Colo. 2016); Saturn Systems, Inc. v. Militare, 252 P.3d 516 (Colo. App. 2011); Hertz v. Luzenac Grp., 576 F.3d 1103 (10th Cir. 2009); Harvey Barnett, Inc. v. Shidler, 338 F.3d 1125 (10th Cir. 2003); Atmel Corp. v. Vitesse S. Corp., 30 P.3d 789 (Colo. App. 2001); Religious Technology Center v. F.A.C.T.NET, Inc., 901 F. Supp. 1519 (D. Colo. 1995); Rivendell Forest Products v. Georgia-Pacific, 28 F.3d 1042 (10th Cir. 1994); Gates Rubber Co. v. Bando Chemical Industries, Ltd., 9 F.3d 823 (10th Cir. 1993); Network v. Boor-Crepeau, 790 P.2d 901 (Colo. App. 1990); Colorado Supply Co., Inc. v. Stewart, 797 P.2d 1303 (Colo. App. 1990); Genworth Financial Wealth Management, Inc. v. McMullan, 721 F. Supp. 2d 122 (D. Conn. 2010); Nationwide Mut. Ins. Co. v. Stenger, 695 F. Supp. 688 (D. Conn. 1988); Premier Lab Supply v. Chemplex Indus, 10 So. 3d 202 (Fla. Dist. Ct. App. 2009); La Bella Vita, LLC v. Shuler, 158 Idaho 799 (Idaho 2015); Walco, Inc. v. Cnty. of Idaho, 357 P.3d 856 (Idaho 2015); Basic American, Inc. v. Shatila, 133 Idaho 726 (Idaho 1999); Am. Ctr. for Excellence in Surgical Assisting Inc. v. Cmty. Coll. Dist. 502, 315 F. Supp. 3d 1044 (N.D. Ill. 2018); Alpha School Bus Co. v. Wagner, 391 Ill. App. 3d 722 (Ill. App. Ct. 2009); System Development Servs. v. Haarmann, 389 Ill. App. 3d 561 (Ill. App. Ct. 2009); Recycled Paper Greetings, Inc. v. Davis, 533 F. Supp. 2d 798 (N.D. Ill. 2008); Fast Food Gourmet, Inc. v. Little Lady Foods, Inc., 542 F. Supp. 2d 849 (N.D. Ill. 2008); Stenstrom Petroleum Services v. Mesch, 375 Ill. App. 3d 1077 (Ill. App. Ct. 2007); U.S. Gypsum Co. v. Lafarge North America, Inc., 508 F. Supp. 2d 601 (N.D. Ill. 2007); Arcor, Inc. v. Haas, 363 Ill. App. 3d 396 (Ill. App. Ct. 2005); Liebert Corp. v. Mazur, 357 Ill. App. 3d 265 (Ill. App. Ct. 2005); Computer Associates Int'l v. Quest Software, Inc., 333 F. Supp. 2d 688 (N.D. Ill. 2004); Learning Curve Toys, Inc. v. Playwood Toys, 342 F.3d 714 (7th Cir. 2003); Delta Medical v. Mid-America Medical, 331 Ill. App. 3d 777 (Ill. App. Ct. 2002); C F Packing Co. v. IBP, Inc., 224 F.3d 1296 (Fed. Cir. 2000); Southwest Whey, Inc. v. Nutrition 101, Inc., 117 F. Supp. 2d 770 (C.D. Ill. 2000); Pope v. Alberto-Culver Co., 296 Ill. App. 3d 512 (Ill. App. Ct. 1998); Colson Co. v. Wittel, 210 Ill. App. 3d 1030 (Ill. App. Ct. 1991);

Service Centers v. Minogue, 180 Ill. App. 3d 447 (Ill. App. Ct. 1989);Amoco Production Co. v. Laird, 622 N.E.2d 912 (Ind. 1993); Ncmic Finance Corp. v. Artino, 638 F. Supp. 2d 1042 (S.D. Iowa 2009); Cemen Tech v. Three D Indus, 753 N.W.2d 1 (Iowa 2008); Sun Media System, Inc. v. KDSM, LLC, 564 F. Supp. 2d 946 (S.D. Iowa 2008); Airfacts, Inc. v. De Amezaga, 909 F.3d 84 (4th Cir. 2018); NaturaLawn of America, Inc. v. West Group, LLC, 484 F. Supp. 2d 392 (D. Md. 2007); Padco Advisors, Inc. v. Omdahl, 179 F. Supp. 2d 600 (D. Md. 2002); Contracts Materials Processing v. Kataleuna GmbH Catalysts, 164 F. Supp. 2d 520 (D. Md. 2001); Home Paramount Pest Control Cos. v. FMC Corp./Agric. Prods. Grp., 107 F. Supp. 2d 684, 694 (D. Md. 2000); Bond v. Polycycle, Inc., 127 Md. App. 365 (Md. Ct. Spec. App. 1999); Trandes Corp. v. Guy F. Atkinson Co., 996 F.2d 655 (4th Cir. 1993); Optic Graphics, Inc. v. Agee, 87 Md. App. 770 (Md. Ct. Spec. App. 1991); Wysong Corporation v. M.I. Industries, 412 F. Supp. 2d 612 (E.D. Mich. 2005); Compuware Corp. v. Serena Software Intern., Inc., 77 F. Supp. 2d 816 (E.D. Mich. 1999); Secure Energy, Inc. v. Coal Synthetics, LLC, 708 F. Supp. 2d 923 (E.D. Mo. 2010); Cerner Corp. v. Visicu, Inc., 667 F. Supp. 2d 1062 (W.D. Mo. 2009); Lyn-Flex West, Inc. v. Dieckhaus, 24 S.W.3d 693 (Mo. Ct. App. 1999); Roton Barrier, Inc. v. Stanley Works, 79 F.3d 1112 (Fed. Cir. 1996); Frantz v. Johnson, 116 Nev. 455 (Nev. 2000); TSG Finishing, LLC v. Bollinger, 767 S.E.2d 870 (N.C. Ct. App. 2014); Philips Electronics North America Corp. v. Hope, 631 F. Supp. 2d 705 (M.D.N.C. 2009); Sunbelt Rentals, Inc. v. Head Engquist Equip, 174 N.C. App. 49 (N.C. Ct. App. 2005); Area Landscaping, L.L.C. v. Glaxo-Wellcome, Inc., 160 N.C. App. 520 (N.C. Ct. App. 2003); Byrd's Lawn Landscapping, Inc. v. Smith, 142 N.C. App. 371 (N.C. Ct. App. 2001); Combs Assocs. v. Kennedy, 147 N.C. App. 362 (N.C. Ct. App. 2001); AK Steel Corp. v. Earley, 809 F. Supp. 2d 1326 (S.D. Ala. 2011); Orthofix, Inc. v. Hunter, 55 F. Supp. 3d 1005 (N.D. Ohio 2014); Jedson Engineering, Inc. v. Spirit Construction Serv., 720 F. Supp. 2d 904 (S.D. Ohio 2010); Erecting v. Genesis Equipment Manufacturing, 649 F. Supp. 2d 702 (N.D. Ohio 2009); Extracorporeal Alliance v. Rosteck, 285 F. Supp. 2d 1028 (N.D. Ohio 2003); Ramco Specialties, Inc. v. Pansegrau, 134 Ohio App. 3d 513 (Ohio Ct. App. 1998); Hoffmann-La Roche Inc. v. Yoder, 950 F. Supp. 1348 (S.D. Ohio 1997); MTG Guarnieri Manufacturing, Inc. v. Clouatre, 239 P.3d 202 (Okla. Civ. App. 2010); Ozburn-Hessey Logistics, LLC v. 721 Logistics, LLC, 13 F. Supp. 3d 465 (E.D. Pa. 2014); Synthes, Inc. v. Emerge Med., Inc., 25 F. Supp. 3d 617 (E.D. Pa. 2014); Bro-Tech Corporation v. Thermax, Inc., 651 F. Supp. 2d 378 (E.D. Pa. 2009); Youtie v. Macy's Retail Holding, Inc., 653 F. Supp. 2d 612 (E.D. Pa. 2009); First Health Group v. National Prescription Adm'rs, 155 F. Supp. 2d 194 (M.D. Pa. 2001); Industrial Insulation Group, LLC v. Sproule, 613 F. Supp. 2d 844 (S.D. Tex. 2009); CDC Restoration & Constr., LC v. Tradesmen Contractors, LLC, 274 P.3d 317 (Utah Ct. App. 2012); Brigham Young Univ. v. Pfizer, Inc., 861 F. Supp. 2d 1320 (D. Utah 2012); USA Power v. Pacificorp, 235 P.3d 749 (Utah 2010); Integrated Direct Marketing, LLC v. May, 129 F. Supp. 3d 336 (E.D. Va. 2015); CSS, Inc. v. Herrington, 306 F. Supp. 3d 857 (S.D.W. Va. 2018); McGough v. Nalco Co., 496 F. Supp. 2d 729 (N.D.W. Va. 2007); Centrifugal Acquisition Corp. v. Moon, 849 F. Supp. 2d 814 (E.D. Wis. 2012); Genzyme Corp. v. Bishop, 463 F. Supp. 2d 946 (W.D. Wis.

2006); Genzyme Corp. v. Bishop, 460 F. Supp. 2d 939 (W.D. Wis. 2006); Nalco Chemical Co. v. Hydro Technologies, Inc., 149 F.R.D. 686 (E.D. Wis. 1993); Minuteman, Inc. v. Alexander, 147 Wis. 2d 842 (Wis. 1989).