



Brian L. Levine is a Managing Director at EY Parthenon, where he leads a group focused on the strategic application of cybersecurity and data privacy to due diligence, integrations, separations, exit readiness, IPO readiness, and investment/PE portfolio management. Prior to joining EY, Mr. Levine served for seven years as Senior Counsel in the U.S. Department of Justice's Computer Crime and Intellectual Property Section ("CCIPS") and National Coordinator for more than 300 federal prosecutors who focus on computer crime and

intellectual property prosecution, as well as the lawful gathering and use of digital evidence. Prior to joining CCIPS, Mr. Levine served as an Assistant Attorney General in the Internet & Technology Bureau at the New York Attorney General's Office; a county prosecutor in Detroit, Michigan; and a civil litigator in Silicon Valley and New York. Mr. Levine has clerked for federal judges in the Southern District of Florida and on the Seventh Circuit. He earned his J.D. from New York University and his B.A. from the University of Pennsylvania.



Eboneé joined BD in August 2014 and has advanced through progressively more responsible positions. As Associate General Counsel - Employment, she provides full service employment law advice and support to all levels of HR professionals, business leaders and managers within the Interventional Segment. In addition, she offers guidance to R&D, Medical/Clinical, Marketing and Global Health. She also supports EMEA. Eboneé also provides guidance to management on acquisition and related integration issues, as well as on company-wide human resource initiatives and best-in-class programs.

She serves as the Co-Lead of BD's Law Group Diversity Internship program. She also led the African Americans at BD (AABD) Associate Resource Group for a two-year term, ending in April 2022. She was featured by *American Healthcare Leader* – *Eboneé Lewis Makes Real Change the Rule* in March 2021. In March 2022, she was also featured in an episode of Littler's Women's History Month podcast series, *Conversation with Women: Perspectives from Littler Alumnae*.

Prior to joining BD, Eboneé served as outside employment counsel to BD while a Shareholder in the Newark office of Littler Mendelson, P.C. While at Littler, Eboneé was selected to be a member of the 2013 class of Fellows for the Leadership Counsel on Legal Diversity program which identifies, trains, and advances the next generation of leaders in the legal profession. Eboneé holds a J.D. from Georgetown University Law Center and a bachelor's degree in Political Science from Syracuse University.



Kendra Ervin is the Deputy Chief for Intellectual Property in the Computer Crime and Intellectual Property Section (CCIPS) of the U.S. Department of Justice. Ms. Ervin leads a group of 15 attorneys dedicated to IP prosecutions and related issues. In her twelve years with CCIPS, Ms. Ervin has prosecuted large-scale, multi-jurisdictional IP crimes; participated in domestic and international IP enforcement training and outreach; and helped to develop and draft legislative and policy initiatives addressing all facets of IP crime. Prior to joining CCIPS, Ms. Ervin was employed as an associate at the law firm of Williams & Connolly, where she specialized in patent litigation. Ms. Ervin also served as a law clerk on the United States Court of Appeals for the Federal Circuit. She earned her J.D. from the University of Virginia School of Law, and her B.S. in Mathematics/Computer Science and Economics from Emory University.



Laura Chubb is an intellectual property partner in Haug Partners' New York office whose practice focuses on patent litigation, related complex commercial disputes, and strategic patent counseling for pharmaceutical and biotechnology companies in the life sciences industry. Laura has experience across a wide range of technologies, including pharmaceuticals, chemicals, and biotechnology. Laura litigates across the country, and provides multi-jurisdictional and global strategy and advice from case inception through resolution. Laura also counsels clients on patent strategy, including pre-litigation activities, freedom-to-operate analysis, portfolio management, and due diligence. Laura has a degree in molecular biology and is admitted to practice before the United States Patent and Trademark Office.

Laura is active in the legal community. She was designated by Haug Partners as a 2022 Fellow in the Leadership Council on Legal Diversity, and was nominated by the firm to participate in the 2017-18 Federal Circuit Bar Association's Global Fellows Program. She co-chairs the Trade Secret Committee of the New York Intellectual Property Law Association. In law school, Laura graduated cum laude and was the Executive Production Editor of the *Indiana International and Comparative Law Review*.



Nick Chambers is an expert in digital investigations and digital forensics. He has over a decade of experience in information technology and investigations, with a focus on digital forensics, cryptocurrency, and eDiscovery. He has served as a digital forensics expert witness in federal and state courts. Prior to joining AlixPartners, Mr. Chambers consulted at a leading eDiscovery firm on digital forensics engagements. He also previously served in the United States Naval Information Warfare Systems Command (NAVWAR) in the technology development group. Mr. Chambers is an EnCase Certified Examiner (EnCE) and a Certified Cryptocurrency Forensic Investigator (CCFI).

Beyond Taking “Reasonable Measures of Protection,” The Protection of Trade Secrets in the Current Era

Giselle Ayala and Anne Rock

Business communications, business models, and cross-border relationships have evolved thanks to the internet and the development of modern technologies. However, together with that progress, trade secrets theft has also changed. In the face of trade secrets theft, owners encounter difficult challenges related to the collection of evidence, prosecution of civil actions against overseas actors, and proper compensation of damages. In fact, nowadays, trade secrets theft can be a matter of state and national concern resulting in enforcement authorities increasing their presence in the courtrooms, leading investigations and prosecutions.

Trade secrets theft may result in civil and criminal liability. While trade secrets owners can bring a lawsuit under the Defense Trade Secrets Act, the Computer Fraud and Abuse Act, common law, and state statutes enacted to protect trade secrets, federal prosecutors may also file criminal charges against individuals and corporations involved in the misappropriation of trade secrets under the Economic Espionage Act. However, there are significant differences between chargeable criminal conduct and actionable civil conduct. Therefore, it is fundamental that trade secrets owners implement strict preventive measures to protect their proprietary information and take an active role in reporting trade secrets theft as soon as possible.

The present article explores recent case law related to the following: i) the requirements to bring a claim under the Defense Trade Secrets Act (DTSA) and the Computer Fraud and Abuse Act (CFAA); ii) the necessity of pleading a trade secrets theft claim with specificity; iii) the challenges that the DTSA present when it comes to arguing unavoidable disclosure and the validity of restrictive covenants; iv) the requirements to bring a claim under the Economic Espionage Act; and v) the reasonable measures of protection that trade secrets owners can take to avoid trade secrets theft or to strengthen their compensation claims.

The requirements to bring a claim under the Defense Trade Secrets Act (DTSA) and the Computer Fraud and Abuse Act

The Defense Trade Secrets Act

Before the enactment of the Defense Trade Secrets Act, in the absence of diversity jurisdiction or an independent basis to establish federal jurisdiction, trade secret owners seeking a remedy for trade secrets theft had no other choice than to file a lawsuit in state court. This resulted in conflicting decisions and conflict of laws issues that delayed any chance of compensation. While the Defense Trade Secrets Act

created a new federal cause of action, it does not prohibit trade secret owners from pursuing a cause of action under existing state trade secret laws. Though, the definition of trade secrets may change from one state to the other.

The Defend Trade Secrets Act created a federal private civil cause of action for trade secrets owners who were victims of espionage or theft and unified the definition of what a trade secret is. Under 18 U.S.C. § 1839(3)¹, a trade secret refers to, “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.”².

In order to bring a viable claim of trade secrets misappropriation, trade secrets owners are required to demonstrate that they took reasonable measures to protect that information which is alleged to be a trade secret under the DTSA. The text of the statute explicitly states, “[...] 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.”³.

This means, that a viable trade secret theft claim requires that the information’s secrecy has value to its owners and the owner must take reasonable measures to keep that information secret. It is the reasonable measures element, in many trade secret litigations, which prevents plaintiffs from establishing their case against defendants. The definition of what reasonable measures are has been one of the most litigated issues relating to trade secrets theft.

In *Turret Labs USA, Inc. v. Cargo Sprint, LLC*,⁴ a recent Second Circuit decision, the court discusses what constitutes reasonable measures. In this case, the Circuit Court affirmed the dismissal of the case because the Plaintiff failed to demonstrate that the information at issue was a “trade secret” under the DTSA and common law, specifically, the Plaintiff did not adequately allege that it took reasonable measures to keep its information secret from third parties.⁵

Turret Labs is the proprietor of a software, Dock EnRoll.⁶ Turret entered into an exclusive licensing agreement with Lufthansa Cargo Americas (“Lufthansa”). The licensing agreement authorized Lufthansa to manage Dock EnRoll and grant access to other users. Turret Labs alleged in their complaint that the defendants gained unfettered access to Dock EnRoll by falsely presenting themselves as freight forwarders to Lufthansa.⁷ However, the complaint was not clear on whether defendant’s access was granted by Lufthansa, or if the defendants used other wrongful means to expand their access after initially receiving login information.⁸

¹ 18 U.S.C.S. § 1839 (LexisNexis, Lexis Advance through Public Law 117-214, approved October 19, 2022)

² *Id.*

³ *Id.*

⁴ *Turret Labs USA, Inc. v. CargoSprint, LLC*, 2022 U.S. App. LEXIS 6070 (2d Cir Mar. 9, 2022, No. 21-952).

⁵ *Id.*

⁶ *Id.*

⁷ *Id.* at *2.

⁸ *Id.* at *2.

The Second Circuit’s analysis turned on what constitutes reasonable measures for protecting a trade secret. The court explained that reasonableness necessarily depends on the nature of the trade secret at issue.⁹ Here, the trade secret at issue was software developed by Turret Labs and licensed to Lufthansa.¹⁰ The Second Circuit explained that where an alleged trade secret consists “primarily, if not entirely,” of a computer software’s functionality—“functionality that is made apparent to all users of the program”—the reasonableness analysis will often focus on who is given access, and on the importance of confidentiality and nondisclosure agreements to maintaining secrecy.¹¹

Basically, from the text of the complaint it was not clear that Lufthansa or any other user of the plaintiff’s software was required to keep plaintiff’s information confidential¹² or that it was prohibited to replicate the software after using it.¹³ This case highlights the importance of trade secrets owners taking reasonable measures, and if seeking to enforce their rights, to clearly plead the measures that were taken.

The Computer Fraud and Abuse Act

Trade Secret owners may also file a federal claim for trade secrets theft under the Computer, Fraud and Abuse Act where the theft has occurred through wrongful use of a computer. Here, it is worth noting that the CFAA provides for a civil cause of action by an employer who has been injured by an individual’s wrongful access to a protected computer. Unlike the DTSA, the CFFA limits the scope of the action and establishes different requirements to establish a viable cause of action, specifically, the trade secret owner must demonstrate that the defendant had no authorization to access the information at the time of the alleged theft.

In *Royal Truck & Trailer Sales & Serv. v Kraft*¹⁴, the plaintiff, employer, failed to satisfy the statutory requirements of the CFFA because its former employees were authorized to access the information in question at the time of the alleged misappropriation. In this case, following the abrupt resignation of two employees, the plaintiff discovered that the employees, prior to resigning, had accessed confidential information from their company-issued computers and cell phones and then utilized the information in violation of company policy. Here, the Court explained:

“The conduct at issue might violate company policy, state law, perhaps even another federal law. But because Royal concedes that the employees were authorized to access the information in question, it has failed to satisfy the statutory requirements for stating a claim under the CFAA.”¹⁵ “The Computer Fraud and Abuse Act’s damages and loss provisions further confirm the Act’s narrow scope. They appear aimed at preventing the typical consequences of hacking, rather than the misuse of corporate information.”¹⁶

The CFAA provides a cause of action for employers to defend their trade secrets. However, in contrast with the DTSA its applicability is more limited.

⁹ *Id.* at *5. (citing *Trim Constr., Inc. v. Gross*, 525 F. Supp. 3d 357, 380 (N.D.N.Y. 2021)).

¹⁰ *Id.*

¹¹ *Id.* (citing *Turret Labs*, 2021 WL 535217, at *4).

¹² *Id.* at *3.

¹³ *Id.*

¹⁴ *Royal Truck & Trailer Sales & Serv. v Kraft*, 974 F3d 756 (6th Cir 2020).

¹⁵ *Id.* at 757.

¹⁶ *Id.* at 761.

The necessity of pleading a trade secrets theft claim with specificity

The necessity of pleading a trade secrets theft claim with specificity has also been an issue frequently discussed by the courts. Enforcing trade secrets in court when there has been a theft presents several challenges to trade secrets owners. Consequently, it is equally important for trade secrets owners to both take preliminary measures to protect their proprietary information and to understand the scope of their trade secrets; with this information, trade secrets owners will be in a better position to make a plea of theft with the proper specificity.

Earlier this year, in *REXA, Inc. v. Chester*¹⁷, the Seventh Circuit reemphasized the need for plaintiffs to identify with particularity a claim of trade secret misappropriation. In this case, the Plaintiff, REXA Inc., filed a lawsuit against an ex-employee of Koso America (Koso), an associated company.¹⁸ Back in 1993, Koso underwent a corporate reorganization to transfer a specific line of business to the Plaintiff. According to the complaint, the defendants misappropriated Koso's information relating to an abandoned prototype, part of the said line of business.¹⁹

The plaintiff's claim for misappropriation of trade secrets was filed under the Illinois Trade Secrets Act ("ITSA"). It is worth noting that in the litigation, the court expressly stated that in order to prevail, the plaintiff must demonstrate "that the information at issue was a trade secret, that it was misappropriated, and that it was used in the defendant's business."²⁰

Following the same logic applied in DTSA cases²¹, the Seventh Circuit affirmed the district court's grant of summary judgment to the defendants.²² Upon review, the Seventh Circuit held that the plaintiff's claim failed "[...] for lack of an identifiable trade secret . . .". Considering that part of the information alleged as a trade secret was actually known in the plaintiff's industry, the claim lacked a fundamental element.²³

The Court emphasized the need for something more than inference to survive the pleading stage, stating, "REXA has not directed us to a case where a court inferred that the misappropriation of trade secrets could plausibly have occurred despite a lack of evidence concerning the defendant's seizure or possession of documents."²⁴

Granting the defendant's motion for summary judgment for the plaintiff's failure to state a trade secret misappropriation claim is not unique to the Seventh Circuit. In *Beijing Neu Cloud Oriental Sys. Tech. Co. v. IBM*²⁵, the Southern District of New York granted a summary judgment motion in favor of the defendants for failure to state a proper trade secrets theft claim.

In this case, the plaintiff filed a complaint under the DTSA, seeking to recover for an alleged misappropriation of their trade secrets by the defendant.²⁶ Defendant, IBM Corporation, filed a motion to

¹⁷ *REXA, Inc. v. Chester*, 42 F.4th 652 (7th Cir 2022).

¹⁸ *Id.*

¹⁹ *Id.* at 653.

²⁰ *REXA, Inc.*, 42 F.4th at 662 (citing *Learning Curve Toys, Inc. v. PlayWood Toys, Inc.*, 342 F.3d 714, 721 (7th Cir. 2003)).

²¹ 18 U.S.C. § 1836(b)(1).

²² *REXA, Inc.*, 42 F.4th 652 at 675.

²³ REXA's claim also fails for lack of an identifiable trade secret because the company concedes that several aspects of the shelved 2002 actuator prototype were and are widely known in the hydraulic-actuator industry. *REXA, Inc.*, 42 F.4th 652, at 664.

²⁴ *Id.* at 665.

²⁵ *Beijing Neu Cloud Oriental Sys. Tech. Co. v. IBM*, 2022 US Dist LEXIS 54348 (SDNY Mar. 25, 2022).

²⁶ *Id.*

dismiss for failure to state a claim.²⁷ The defendant's motion was granted.²⁸ The main facts of the complaint are based on a purchase agreement entered into between the parties. Neu Cloud, the plaintiff, entered into an agreement with IBM, the defendant, for the purchase of equipment that would be integrated with Neu Cloud's own products. "Pursuant to that agreement, Neu Cloud submitted to IBM China bid requests, which included Neu Cloud's customer information."²⁹

To the point of making a plea for trade secrets theft with specificity, the court stated, "[h]ere, Plaintiffs have done little more than plead 'broad categories of information,' which is legally insufficient to state a claim. [...] The Complaint alleges that "customer information" is a trade secret and asserts that such information is a trade secret by reciting the statutory elements without providing additional details."³⁰

The court was emphatic that the Second Circuit district courts "require that allegations of misappropriation plead the existence of trade secrets with sufficient specificity to inform the defendants of what they are alleged to have misappropriated."³¹ In this case, the plaintiff failed to plead facts that explain how the defendant misappropriated trade secrets, and how plaintiffs' trade secrets were developed or generated. The plaintiffs' argument that the defendant benefitted from the use of the trade secrets, alone, was insufficient to establish the misappropriation prong under the DTSA.³²

Rexa and *Neu Cloud* highlight the frequent dilemma that plaintiffs face in trade secrets litigation. On the one hand, to survive the pleading stage, plaintiffs must identify the existence of the trade secret and the unlawful act of misappropriation. On the other hand, plaintiffs must be careful of how much information they provide in their pleading and consider the consequences of making excessive disclosures. In this context, defendants have shown frequent success at the summary judgment level.³³

The challenges that the DTSA presents when it comes to arguing unavoidable disclosure and the validity of restrictive covenants

The proper defense of a trade secrets theft claim requires specific pleadings regarding the definition of the trade secret and the act of misappropriation. However, in the context of employment agreements, there is an additional challenge for trade secret owners defending a trade secret theft claim under the DTSA; this is defending the validity of the inevitable disclosure doctrine, NDAs, and restrictive covenants, which are intended to protect owners' proprietary information.

In the context of trade secrets litigation between employers and employees, especially regarding claims that arise when an employee changes jobs, trade secrets owners usually argue the unavoidable disclosure of their proprietary information by the former employee. Under the inevitable disclosure doctrine, trade secret owners are allowed to "prove a claim of trade secret misappropriation by demonstrating that defendant's new employment will inevitably lead him to rely on the plaintiff's trade secrets."³⁴

²⁷ *Id.*

²⁸ *Id.*

²⁹ *Id.*

³⁰ *Beijing Neu Cloud Oriental Sys. Tech. Co.*, 2022 U.S. Dist. LEXIS 54348, at *11 (S.D.N.Y. Mar. 25, 2022)

³¹ *Id.* at *4.

³² *Id.*

³³ 18 USCS § 1836 (LexisNexis, Lexis Advance through Public Law 117-214, approved October 19, 2022)

³⁴ *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262, 1269 (7th Cir. 1995).

The discussion about the applicability of the inevitable disclosure doctrine comes from a specific provision in the DTSA, which states that a court may not grant an injunction to “prevent a person from entering into an employment relationship”. Moreover, the DTSA requires that prior to granting an injunction the plaintiff is required to provide “evidence of threatened misappropriation and not merely on the information the person knows.”³⁵ Finally, according to the DTSA an injunction is also prohibited when it is conflicting with an applicable state law.

The DTSA was created in part to serve as a single standard to litigate trade secrets theft, in other words, to create a common understanding of what is required to defend a trade secrets theft claim, with clear rule and predictability to all litigants.³⁶ However, to this date, courts’ position regarding the applicability of the inevitable disclosure doctrine is split.

Early this year, in *Kinship Partners, Inc. v. Embark Veterinary, Inc.*³⁷, the United States District Court for the District of Oregon, denied the plaintiff’s motion for a preliminary injunction intended to prevent a former employee from changing to a new position with plaintiff’s main competitor. The court noted that the plaintiff did not demonstrate a likelihood of succeeding on the merits, the effective existence of irreparable harm risk, and the balance of the equities did not tip in his favor.³⁸

Additionally, the district court noted that it has been the Oregon legislature’s purpose to promote employee freedom and mobility. The court recognized that injunctive relief has been granted in specific cases in the past, like in *Phoseon Tech., Inc. v. Heathcote*³⁹, where the plaintiff’s request for an injunction was granted because of an existing noncompete agreement, but then stated that it was unlikely that Oregon would adopt a general applicability of the inevitable disclosure doctrine, because granting such relief could undermine Oregon’s public interest goals.

Illinois, notably, has recognized the applicability of the inevitable disclosure doctrine. In *GE v Uptake Tech., Inc.*⁴⁰ the Illinois Northern District Court recognized that Illinois allows the inevitable disclosure doctrine to support a plaintiffs’ claim of trade secrets theft and that a DTSA claim based on inevitable disclosure may survive a motion to dismiss. Delaware has also recognized the inevitable disclosure doctrine, in *W.L. Gore & Assoc. v Wu*⁴¹, the court explained that “[a] court may limit a defendant from working in a particular field if his doing so poses a substantial risk of the inevitable disclosure of trade secrets.”⁴² Finally, in Pennsylvania, in *Jazz Pharms., Inc. v Synchrony Group, LLC*⁴³, the court recognized that, “[t]he Third Circuit has held that where an employee’s work for a new employer substantially overlaps with work for a former employer, based on the same role, industry, and geographic region, a district court

³⁵ 18 USCS § 1836 (LexisNexis, Lexis Advance through Public Law 117-214, approved October 19, 2022)

³⁶ Danielle A. Duszczyszyn and Daniel F. Roland. Three Years Later: How the Defend Trade Secrets Act Complicated the Law Instead of Making It More Uniform. Aug. 2019. <https://www.finnegan.com/en/insights/articles/three-years-later-how-the-defend-trade-secrets-act-complicated-the-law-instead-of-making-it-more-uniform.html>

³⁷ *Kinship Partners, Inc. v Embark Veterinary, Inc.*, 2022 US Dist LEXIS 2804 (D Or Jan. 3, 2022, No. 3:21-cv-01631-HZ).

³⁸ “Plaintiff alleges, but cannot demonstrate, that Smith’s role at Embark is substantially similar to his prior role at Kinship [...] Next, Plaintiff presents no facts that show Smith would necessarily disclose Kinship’s trade secrets to fulfill his job duties at Embark. [...] Plaintiff cannot show irreparable harm because there is no evidence that Smith acted in bad faith or has breached his Confidentiality Agreement [...] Plaintiff cannot show its trade secrets are under threat of misappropriation because it relies on a legal theory that is unavailable in Oregon. *Id.*”

³⁹ *Phoseon Tech., Inc. v Heathcote*, 2019 US Dist LEXIS 221633 (D Or Dec. 27, 2019, No. 3:19-cv-2081-SI).

⁴⁰ *GE v Uptake Tech., Inc.*, 394 F Supp 3d 815 (ND Ill 2019).

⁴¹ *W.L. Gore & Assocs. v. Wu*, Civil Action No. 263-N, 2006 Del. Ch. LEXIS 176 (Del. Ch. Sep. 15, 2006)

⁴² *Id.* at *59.

⁴³ *Jazz Pharms., Inc. v Synchrony Group, LLC*, 343 F Supp 3d 434 (ED Pa 2018).

may conclude that those employees would likely use confidential information to the former employer's detriment."⁴⁴.

However, it seems like the tendency is moving against a general recognition of the inevitable disclosure doctrine. In *Idexx Lab'ys v. Bilbrough*⁴⁵, the District Court of Maine, despite recognizing that there is not judicial consensus⁴⁶ as to the applicability of the inevitable disclosure doctrine under the DTSA, expressly stated that, "[t]o the extent there is an ambiguity in the statute, a review of the development of the statute suggests Congress did not intend the doctrine to apply to DTSA claims. [...] In sum, based on the plain language of the statute, the inevitable disclosure doctrine does not apply to claims brought pursuant to DTSA."⁴⁷.

In *UCAR Tech. (USA) Inc. v. Yan Li*⁴⁸, the Northern District of California struck DTSA allegations that relied on the inevitable disclosure doctrine because, "California courts have resoundingly rejected claims based on the 'inevitable disclosure' theory"⁴⁹. In *Prime Therapeutics LLC v. Beatty*⁵⁰, the District Court of Minnesota expressed in a foot note, "[...] the Court has identified only one case from this District finding inevitable disclosure of trade secrets . . ."⁵¹ and denied plaintiff's request for injunctive relief due to lack of evidentiary support.

For employers, the fate of the inevitable disclosure doctrine remains unclear due to the split of positions between district courts. Additionally, recently this year, Colorado and Washington issued state statutes that restrict the enforceability of restrictive covenants imposed by employers. A growing number of states has taken judicial or legislative measures to limit, or even ban, the applicability of covenants that limit employee's mobility⁵².

The requirements to bring a claim under the Economic Espionage Act

Together with the DTSA, the Economic Espionage Act (EEA), a criminal federal statute, gives trade secrets owners another option to take action against trade secrets theft. Before the enactment of the DTSA, it was uncommon for trade secrets owners to get involved in the criminal investigation of trade secrets theft. However, DTSA brought the topic of trade secrets misappropriation to the first row and raised awareness of the necessity of mutual collaboration between trade secrets owners and enforcement authorities. Similar, to the DTSA, the EEA broadly defines the term "trade secret" to include all types of information that the owner has taken reasonable measures to keep secret and that itself has independent economic value⁵³.

Trade secrets theft can result in criminal liability. However, not every act of trade secrets misappropriation is investigated or pursued by the Department of Justice (DOJ). Before initiating a criminal investigation, the DOJ considers several factors, including, the scope of the criminal activity, the existence of evidence of involvement by a foreign instrumentality, the degree of economic injury to the trade secret owner, the

⁴⁴ *Id.* at 446.

⁴⁵ *Idexx Lab'ys v Bilbrough*, 2022 US Dist LEXIS 136676 (D Me Aug. 2, 2022, No. 2:22-cv-00056-JDL).

⁴⁶ *Id.* (citing *Sunbelt Rentals, Inc. v. McAndrews*, 552 F. Supp. 3d 319, 331 (D. Conn. 2021)).

⁴⁷ *Id.*

⁴⁸ *UCAR Tech. (USA) Inc. v. Yan Li*, No. 5:17-CV-01704-EJD, 2017 WL 6405620.

⁴⁹ *Id.*

⁵⁰ *Prime Therapeutics LLC v Beatty*, 354 F Supp 3d 957 (D Minn 2018)

⁵¹ *Id.*

⁵² Mark S. Goldstein and Noah S. Oberlander. What does the future hold for restrictive covenant agreements in the U.S.? Reuters. Oct. 21, 2021. <https://www.reuters.com/legal/legalindustry/what-does-future-hold-restrictive-covenant-agreements-us-2021-10-01/>.

⁵³ 18 U.S.C.S. § 1839 (LexisNexis, Lexis Advance through Public Law 117-214, approved October 19, 2022)

type of trade secret misappropriated, the effectiveness of available civil remedies and the potential value of the prosecution.⁵⁴

The EEA contains two separate provisions that criminalize the theft of trade secrets. The first, 18 U.S.C. § 1831, prohibits the theft of trade secrets for the benefit of a foreign government, instrumentality, or agent, and is punishable by up to 15 years' imprisonment and a \$5,000,000 fine. The second, 18 U.S.C. § 1832, prohibits the commercial theft of trade secrets to benefit someone other than the owner, and is punishable by up to ten years' imprisonment and a \$250,000 fine. The penalties are higher for defendants who are companies.

The EEA also provides special provisions to ensure that the confidentiality of trade secret information is preserved during the course of criminal proceedings. Specifically, the statute expressly states that courts “[...] shall enter such orders and take such action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws.”⁵⁵

Recently, criminal investigations under the EEA have resulted in substantial judgments. In *USA v. You et al*⁵⁶, a chemist was convicted of conspiracy to commit trade secret theft, conspiracy to commit economic espionage, possession of stolen trade secrets, and sentenced to 14 years in prison, a \$200,000 fine and a \$10,000 restitution. On the civil side of this case, in *Appian Corp. v. Pegasystems Inc.*⁵⁷, a Virginia jury awarded the plaintiff \$2.04 billion in damages for trade secret misappropriation.

Practitioners should be mindful that there is a large disparity in sentencing by federal courts for trade secret theft. This year, in California in a trade secrets case exceeding \$101 million, a biotech CEO was sentenced to 12 months in prison, while in Florida, for a trade secrets theft amounting to \$135,000, a certified teacher was sentenced to 10 months, and in New York, for a trade secrets theft amounting to \$1.4 million, an engineer was sentenced to 24 months.⁵⁸

In criminal prosecution, sentencing is determined by the “intended loss”. In *USA v. You et al*, the court explained that the “intended loss” means the loss the defendant purposely sought to cause and not the loss that the defendant knew would result from his conduct. The court stated, “[...] courts in multiple circuits have found that in trade secrets cases, [the intended loss] turns upon how much loss the defendant actually intended [...] regardless of whether the loss actually materialized [...]”⁵⁹.

⁵⁴ Economic Espionage Act of 1996 (18 U.S.C. §§ 1831-1837)—Prosecutive Policy, Chapter 9-59.100. <https://www.justice.gov/jm/jm-9-59000-economic-espionage#:~:text=It%20was%20passed%20in%20recognition,this%20important%20area%20of%20law.>

⁵⁵ 18 U.S.C. § 1835(a); see also Levine & Flowers, How Prosecutors Protect Trade Secrets, 38 Am. J. Trial Advoc. 461 (2014-2015).

⁵⁶ *USA v. You et al*. 2:19cr14.

⁵⁷ *Appian Corp. v. Pegasystems Inc.*, No. 2020-07216 (Va. Cir. Ct. Fairfax Cty. May 9, 2022).

⁵⁸ Steven H. Lee. Sentencing Disparities Can Lead to Increased Uncertainty for Victim Companies of Trade Secret Theft. <https://lewisbrisbois.com/newsroom/legal-alerts/sentencing-disparities-can-lead-to-increased-uncertainty-for-victim-companies-of-trade-secrets-theft#:~:text=Legal%20Alerts-,Sentencing%20Disparities%20Can%20Lead%20to%20Increased%20Uncertainty%20for%20Victim%20Companies,billion%20and%20%2024600%20billion%20annually.>

⁵⁹ *USA v. You et al* 2:19-cr-00014-JRG-CRW. PACER Doc. No. 420. (citing *United States v. Xue*, No. 16-22, 2020 U.S. Dist. LEXIS 173410, at *40-*42 (E.D. Pa. Sept. 22, 2020)) (citing *United States v. Pu*, 814 F.3d 818, 824 (7th Cir. 2016) (citations partially omitted)).

In this context, the DOJ has developed a longstanding policy promoting communication and coordination between federal prosecutors and civil attorneys handling trade secret theft actions⁶⁰.

Reasonable measures of protection that trade secrets owners can take to avoid trade secrets theft or to strengthen their compensation claims

Prosecution of trade secrets theft presents many challenges to trade secrets owners, not only because of the procedural requirements of the action to survive the pleadings stage, but also because trade secrets owners must demonstrate the existence of the trade secret and the prior practice of taking proper measures to protect their proprietary information. Considering this, here is a non-comprehensive list of good practices that trade secret owners can implement to protect themselves and improve their possibilities of recovery in the case of a misappropriation.

- In the case of a suspected theft of trade secrets, any internal investigation or surveillance of the suspect, or a competitor believed to be using the stolen information, should be recorded. Records of any interviews with suspects or witnesses should be made by tape or in writing. The pertinent confidentiality agreements, security policies, and access logs should also be gathered and maintained to facilitate review and reduce the risk of deletion or destruction.⁶¹
- Any physical, documentary, or digital evidence acquired in the course of an internal investigation should be preserved for later use in a legal proceeding.⁶²
- If the computer of an employee suspected of stealing trade secrets has been seized, any forensic analysis should be performed on a copy of the data, or “digital image,” to refute claims that the evidence has been altered or corrupted.
- Early referral to law enforcement is the best way to ensure that evidence of an intellectual property crime is properly secured and that all investigative avenues are fully explored, such as the execution of search warrants and possible undercover law enforcement activities. To be ready to act urgently when a theft occurs, a company should develop a relationship with their local FBI field office and also familiarize themselves with the DOJ’s guide for reporting intellectual property crime.⁶³ Not only will the DOJ’s guide assist a company in making any criminal referral, but if followed, a company will likely have more success even in the civil arena because it will have thought through identification of its trade secret and what measures to take for protection of it⁶⁴.

⁶⁰ Jeffrey A Pade and Anand B. Patel. Criminal Considerations In Trade Secrets Disputes. Part One of a Three-Part Series. Oct. 2022. <https://www.lawjournalnewsletters.com/2022/10/01/criminal-considerations-in-trade-secrets-disputes/?sreturn=20221001215852>

⁶¹ REPORTING INTELLECTUAL PROPERTY CRIME. A Guide for Victims of Copyright Infringement, Trademark Counterfeiting, and Trade Secret Theft. Third Edition. U.S. Department of Justice | Computer Crime and Intellectual Property Section. October 2018. <https://www.justice.gov/criminal-ccips/file/891011/download>

⁶² *Id.*

⁶³ *Id.*

⁶⁴ *Id.*



Neutral

As of: November 2, 2022 2:12 AM Z

[Turret Labs USA, Inc. v. CargoSprint, LLC](#)

United States Court of Appeals for the Second Circuit

March 9, 2022, Decided

21-952

Reporter

2022 U.S. App. LEXIS 6070 *; 2022 WL 701161

TURRET LABS USA, INC., Plaintiff-Appellant,
v. CARGOSPRINT, LLC, JOSHUA WOLF,
Defendants-Appellees.

Notice: PLEASE REFER TO *FEDERAL RULES OF APPELLATE PROCEDURE RULE 32.1* GOVERNING THE CITATION TO UNPUBLISHED OPINIONS.

Prior History: [*1] Appeal from a judgment of the United States District Court for the Eastern District of New York (Komitee, J.).

[Turret Labs USA, Inc. v. CargoSprint, LLC, 2021 U.S. Dist. LEXIS 27838, 2021 WL 535217 \(E.D.N.Y., Feb. 12, 2021\)](#)

Core Terms

trade secret, confidentiality, reasonable measure, users, software, alleges, district court, secret, misappropriation, nondisclosure, secrecy

Case Summary

Overview

HOLDINGS: [1]-In an appeal from a judgment dismissing plaintiff's claims for misappropriation of a trade secret under the Defend Trade Secrets Act (DTSA), [18 U.S.C.S. § 1836\(b\)](#), and common-law misappropriation of a trade secret, plaintiff did

not plausibly allege that defendants misappropriated a trade secret under the DTSA, [18 U.S.C.S. § 1839\(3\)\(A\)](#) because plaintiff did not plead that it had confidentiality or nondisclosure agreements in place with cargo company or other users of plaintiff's software, nor did it allege that cargo company was obligated to limit access to the software to freight forwarders that were themselves bound to respect the secrecy of plaintiff's information.

Outcome

Judgment affirmed.

LexisNexis® Headnotes

Civil Procedure > Appeals > Standards of Review > De Novo Review

Civil Procedure > ... > Defenses, Demurrers & Objections > Motions to Dismiss > Failure to State Claim

Civil
Procedure > ... > Pleadings > Complaints > Requirements for Complaint

[HN1](#) [↓] **Standards of Review, De Novo Review**

An appellate court reviews de novo the district court's dismissal of a complaint pursuant to [Fed. R. Civ. P. 12\(b\)\(6\)](#). To survive a motion to

dismiss brought under [Fed. R. Civ. P. 12\(b\)\(6\)](#), a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face. Appellate courts are required to accept all well-pleaded factual allegations in the complaint as true and construe all reasonable inferences that can be drawn from the complaint in the light most favorable to the plaintiff, but an appellate court need not credit conclusory allegations.

Trade Secrets Law > Misappropriation
Actions > Elements of
Misappropriation > Confidentiality

Trade Secrets Law > Trade Secret
Determination Factors > Economic Value

Trade Secrets Law > Trade Secret
Determination Factors > Generally Known

Trade Secrets Law > Trade Secret
Determination Factors > Ready Availability

Trade Secrets Law > Misappropriation
Actions > Elements of
Misappropriation > Existence & Ownership

[HN2](#) [↓] **Elements of Misappropriation, Confidentiality**

Under [§ 1836](#) of the Defend Trade Secrets Act (DTSA), the owner of a trade secret that is misappropriated may bring a civil action if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce. [18 U.S.C.S. § 1836\(b\)\(1\)](#). For financial, business, scientific, technical, economic, or engineering information to constitute a trade secret, two factors must be satisfied: (A) the owner must have taken reasonable measures to keep such information secret; and (B) the information must derive 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. [18 U.S.C.S. § 1839\(3\), \(3\)\(A\)-\(B\)](#).

Business & Corporate
Compliance > ... > Trade Secrets
Law > Protection of Secrecy > Duty to
Safeguard

Trade Secrets Law > Misappropriation
Actions > Elements of
Misappropriation > Confidentiality

Labor & Employment Law > ... > Conditions
& Terms > Trade Secrets & Unfair
Competition > Trade Secrets

Trade Secrets Law > Misappropriation
Actions > Elements of
Misappropriation > Existence & Ownership

[HN3](#) [↓] **Protection of Secrecy, Duty to Safeguard**

The Defend Trade Secrets Act (DTSA) gives scant guidance on what constitutes reasonable measures to keep information secret. But given that trade secrets may appear in a wide variety of forms and types, [18 U.S.C.S. § 1839\(3\)](#), what measures are reasonable must depend in significant part on the nature of the trade secret at issue. Where an alleged trade secret consists primarily, if not entirely, of a computer software's functionality, functionality that is made apparent to all users of the program, the reasonableness analysis will often focus on who is given access, and on the importance of confidentiality and nondisclosure agreements to maintaining secrecy.

Labor & Employment Law > ... > Conditions
& Terms > Trade Secrets & Unfair
Competition > Trade Secrets

Trade Secrets Law > Misappropriation
Actions > Elements of
Misappropriation > Confidentiality

[HN4](#) Trade Secrets & Unfair Competition, Trade Secrets

Providing alleged trade secrets to third parties does not undermine a trade-secret claim, so long as the information is provided on an understanding of confidentiality.

Business & Corporate
Compliance > ... > Trade Secrets
Law > Protection of Secrecy > Duty to
Safeguard

Trade Secrets Law > Misappropriation
Actions > Elements of
Misappropriation > Confidentiality

[HN5](#) Protection of Secrecy, Duty to Safeguard

Under New York common law, owner of a trade secret must take reasonable measures to protect its secrecy.

Counsel: For Plaintiff-Appellant: Leslie R. Bennett (Leslie R. Bennett LLC), Melville, NY.

For Defendants-Appellees: R. Dale Grimes, Virginia M. Yetter, and Nicholas J. Goldin (Bass, Berry & Sims, PLC), Nashville, TN; Michael Dashefsky (Bass, Berry & Sims, PLC), Washington, D.C.; Joseph A. Matteo (Barnes & Thornburg LLP), New York, NY.

Judges: Present: DEBRA ANN LIVINGSTON, Chief Judge, AMALYA L. KEARSE, EUNICE C. LEE, Circuit Judges.

Opinion

SUMMARY ORDER

UPON DUE CONSIDERATION, IT IS HEREBY ORDERED, ADJUDGED, AND DECREED that the judgment of the district court is **AFFIRMED**.

Plaintiff-Appellant Turret Labs USA, Inc. ("Turret Labs") appeals from the district court's **March** 22, 2021 judgment dismissing its second amended complaint ("SAC") for failure to state a claim pursuant to [Federal Rule of Civil Procedure 12\(b\)\(6\)](#). [Turret Labs USA, Inc. v. CargoSprint, LLC, No. 19-CV-6793, 2021 U.S. Dist. LEXIS 27838, 2021 WL 535217, at *1 \(E.D.N.Y. Feb. 12, 2021\)](#). Turret Labs alleges that Defendants-Appellees CargoSprint, LLC and its chief executive officer, Joshua Wolf, improperly gained access to Turret Labs' software, Dock EnRoll, and reverse engineered it to create their own competing program.¹ Turret Labs claims misappropriation of a trade secret under the [Defend Trade Secrets Act \("DTSA"\)](#), [***2**] [18 U.S.C. § 1836\(b\)](#), and common-law misappropriation of a trade secret.² The district court dismissed these trade secret claims, ruling that Turret Labs failed as a matter of law to plead that Dock EnRoll was a "trade secret" under the DTSA and common law because the Plaintiff-Appellant did not adequately allege that it took reasonable measures to keep its information secret from third parties. [Turret Labs, 2021 U.S. Dist. LEXIS 27838, 2021 WL](#)

¹Dock EnRoll is an "air cargo ground handling control application that allows for payment of fees and scheduling of shipments based on synchronized real-time United States Customs release notifications, [and] was the first software of its kind at the time." SAC ¶ 17.

²The SAC also brings claims for common-law unfair competition, conversion, and defamation, as well as fraud in connection with computers under the [Computer Fraud and Abuse Act \("CFAA"\)](#), [18 U.S.C. § 1030](#). The district court dismissed the unfair competition, conversion, and CFAA claims, [Turret Labs, 2021 U.S. Dist. LEXIS 27838, 2021 WL 535217, at *6-7](#), and the parties voluntarily agreed to dismiss the defamation claim with prejudice shortly thereafter. Turret Labs does not pursue these claims on appeal.

[535217](#), at *4-6. We assume the parties' familiarity with the underlying facts, the procedural history of the case, and the issues on appeal.

* * *

HN1^[↑] We review *de novo* the district court's dismissal of Turret Labs' SAC pursuant to [Rule 12\(b\)\(6\)](#). See [Pettaway v. Nat'l Recovery Sols., LLC](#), 955 F.3d 299, 304 (2d Cir. 2020). To survive a motion to dismiss brought under [Rule 12\(b\)\(6\)](#), a complaint "must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" [Ashcroft v. Iqbal](#), 556 U.S. 662, 678, 129 S. Ct. 1937, 173 L. Ed. 2d 868 (2009) (quoting [Bell Atl. Corp. v. Twombly](#), 550 U.S. 544, 570, 127 S. Ct. 1955, 167 L. Ed. 2d 929 (2007)). We are "required to accept all well-pleaded factual allegations in the complaint as true" and "construe all reasonable inferences that can be drawn from the complaint in the light most favorable to the plaintiff," but we need not credit conclusory allegations. [Lynch v. City of New York](#), 952 F.3d 67, 74-75 (2d Cir. 2020) (internal quotation marks and citations omitted).

HN2^[↑] Under [Section 1836 of the DTSA](#), the owner of a "trade secret that is misappropriated may bring a civil action . . . if the trade [*3] secret is related to a product or service used in, or intended for use in, interstate or foreign commerce." [§ 1836\(b\)\(1\)](#). For "financial, business, scientific, technical, economic, or engineering information" to constitute a "trade secret," two factors must be satisfied: (A) the owner must have "taken reasonable measures to keep such information secret"; and (B) the information must "derive[] 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" [18 U.S.C. § 1839\(3\)](#), [\(3\)\(A\)-\(B\)](#). Turret Labs argues that the district court erred in concluding that it failed adequately to allege that it took reasonable measures to protect Dock EnRoll's secrecy. For the following reasons, we disagree.

Turret Labs alleges that after developing Dock EnRoll, it entered into a joint venture agreement and an exclusive licensing agreement with Lufthansa Cargo Americas ("Lufthansa"), which authorized Lufthansa to manage Dock EnRoll and grant access to other users. SAC ¶ 21(f) ("User Access for Dock EnRoll is managed by Lufthansa only[] and no other party has access [*4] without Lufthansa's authority"); SAC ¶ 21(j) (pleading that Turret Labs "assign[ed] to Lufthansa the right to vet users and grant access"). The SAC alleges that Defendants-Appellees gained unfettered access to Dock EnRoll by falsely presenting themselves as freight forwarders to Lufthansa.³ It is not clear from the SAC, however, whether such unfettered access was granted by Lufthansa, or if Defendants-Appellees used other wrongful means to expand their access after initially receiving login information.⁴ Turret Labs pleads, without explanation, that Defendants-Appellees were "given unfettered access to all corners of the Dock EnRoll platform that, based on Lufthansa's protocols, no freight forwarder or other user would have been granted access to, and it was only due to Defendants' wrongful

³ "Freight forwarders" are "the entities that arrange for the storage and shipping of merchandise on behalf of shippers." SAC ¶ 16.

⁴ Turret Labs alternatively alleges that Defendants-Appellees gained access by "[u]sing a pre-approved access through Damco or other authorized freight forwarders [to] log[] in to the system" SAC ¶ 24(b). Turret Labs alleges nothing further regarding "Damco," however, or how access to an approved freight forwarder's login information was used to obtain unfettered access "above and beyond what authorized [freight forwarders] would be entitled to access" See SAC ¶ 35.

actions that they were able to obtain such greater access to the platform."⁵ SAC ¶ 31. Such "expansive unauthorized access to [Dock EnRoll] and confidential information contained therein allowed [Defendants-Appellees] to reverse engineer the software," SAC ¶ 34, and create a program that is "identical to Dock EnRoll, particularly the scheduling system," SAC ¶ 35.

HN3 [↑] The DTSA gives scant guidance on [*5] what constitutes "reasonable measures" to keep information secret. But given that trade secrets may appear in a wide variety of "forms and types," § 1839(3), "[w]hat measures are 'reasonable' must depend in significant part on the nature of the trade secret at issue," see *Exec. Trim Constr., Inc. v. Gross*, 525 F. Supp. 3d 357, 380 (N.D.N.Y. 2021). We agree with the district court that where an alleged trade secret consists "primarily, if not entirely," of a computer software's functionality—"functionality that is made apparent to all users of the program"—the reasonableness analysis will often focus on who is given access, and on the importance of confidentiality and nondisclosure agreements to maintaining secrecy. *Turret Labs*, 2021 U.S. Dist. LEXIS 27838, 2021 WL 535217, at *4; see also *Mason v. Amtrust Fin. Servs., Inc.*, 848 F. App'x 447, 450 (2d Cir. 2021) (holding that plaintiff's failure to "execut[e] a nondisclosure or licensing agreement or . . . stipulat[e] in his employment contract that the [software] was his proprietary information" evidenced that he

"had not taken reasonable measures to protect his information"); *Inv. Sci., LLC v. Oath Holdings Inc.*, No. 20 Civ. 8159, 2021 U.S. Dist. LEXIS 151076, 2021 WL 3541152, at *3 (S.D.N.Y. Aug. 11, 2021) (concluding that the plaintiff did not employ reasonable measures to protect its claimed trade secrets because, among other reasons, the plaintiff "concede[d] that it did not require [the defendant] to sign a confidentiality agreement before sharing the contents of the [product]"); [*6] *Exec. Trim*, 525 F. Supp. 3d at 380; *Charles Ramsey Co., Inc. v. Fabtech-NY LLC*, No. 1:18-CV-0546, 2020 U.S. Dist. LEXIS 9348, 2020 WL 352614, at *15 (N.D.N.Y. Jan. 21, 2020) (collecting cases); *Mintz v. Mktg. Cohorts, LLC*, No. 18-CV-4159, 2019 U.S. Dist. LEXIS 124374, 2019 WL 3337896, at *6 (E.D.N.Y. July 25, 2019) (dismissing a DTSA claim because plaintiff "did not require defendants to sign a non-disclosure agreement nor any sort of covenant to protect the passwords").

This observation is consistent with those of our sister circuits. See, e.g., *Farmers Edge Inc. v. Farmobile, LLC*, 970 F.3d 1027, 1033 (8th Cir. 2020) (holding that under the DTSA, a company that, "without a confidentiality agreement and without other policies or practices for safeguarding secrets . . . shared the relevant information with a third-party who had no obligation to keep it confidential . . . did not take reasonable steps to safeguard its trade secrets"); *InteliClear, LLC v. ETC Glob. Holdings, Inc.*, 978 F.3d 653, 660 (9th Cir. 2020) (holding, under the DTSA, that the plaintiff took "reasonable measures" by "encrypt[ing] and compil[ing] its source code and requir[ing] licensees to agree to confidentiality," as "[c]onfidentiality provisions constitute reasonable steps to maintain secrecy"); *VBS Distribution, Inc. v. Nutrivita Lab'ys, Inc.*, 811 F. App'x 1005, 1009 (9th Cir.), cert. denied, 141 S. Ct. 454, 208 L. Ed. 2d 145 (2020) ("**HN4** [↑] Providing alleged trade secrets to third parties does not

⁵ Turret Labs alleges that a freight forwarder's access to Dock EnRoll would generally "allow such forwarder to be able to see information for airway bills assigned to that [particular] forwarder," SAC ¶ 32, but that Defendants-Appellees were "able to gain access to the airway bill information of multiple freight forwarders," providing them information such as the name of the shipper, consignee name, nature of the goods, weight, volume and customs release information, "which is proprietary information for the specific freight forwarder," SAC ¶ 33.

undermine a trade-secret claim, so long as the information was provided on an understanding of confidentiality." (internal quotation marks and citation omitted)).

Notably absent from Turret Labs' SAC is any specific allegation that Lufthansa or any other user of Dock EnRoll was required [*7] to keep Turret Labs' information confidential. Turret Labs does not plead that it had confidentiality or nondisclosure agreements in place with Lufthansa or other users of Dock EnRoll. Nor does it allege that Lufthansa was obligated to limit access to the software to freight forwarders that were themselves bound to respect the secrecy of Turret Labs' information. Although the SAC alleges generally that Lufthansa's internal guidelines dictated the terms of use, there is no allegation that these guidelines contractually obligated users to keep the software, its client-facing functionality, or its internal mechanics confidential. And without confidentiality or nondisclosure agreements in this context, it is not apparent from the SAC that *any* user could not simply replicate the software after using it.

Turret Labs argues that, regardless, its extensive list of security measures for Dock EnRoll, as pled in the SAC, plausibly constitutes "reasonable measures" to keep its information secret. See [§ 1839\(3\)\(A\)](#). The SAC pleads, among other things, that Dock EnRoll's physical servers were kept in monitored cages within a data center with restricted access and that access to the software was limited to those [*8] with usernames and passwords approved by Lufthansa. SAC ¶ 21. But secured physical servers are largely irrelevant where users such as Defendants-Appellees could simply be given access by Lufthansa and view and replicate Dock EnRoll's functionality. And, again, the SAC is silent regarding any obligation on Lufthansa's part to protect proprietary information by granting access only to legitimate freight forwarders

bound by confidentiality agreements. The SAC implies (but does not allege) that Defendants-Appellees hacked into the software to obtain unfettered access to Dock EnRoll's algorithms and other internal mechanics after getting login information from Lufthansa. But Turret Labs has failed to plead how any of its security measures might have prevented such an unwanted intrusion.

In the absence of nonconclusory allegations that it took reasonable measures to keep its information secret, Turret Labs has not plausibly alleged that Defendants-Appellees misappropriated a "trade secret" under the DTSA. See [§ 1839\(3\)\(A\)](#). Turret Labs' common-law misappropriation claim is inadequately pled for the same reason. See [Defiance Button Mach. Co. v. C & C Metal Prod. Corp.](#), 759 F.2d 1053, 1063 (2d Cir. 1985) (noting that [HN5](#) [↑] under New York common law, owner of a trade secret must take "reasonable [*9] measures to protect its secrecy" (internal quotation marks omitted)); [Mason](#), 848 F. App'x at 450-51. Accordingly, the district court did not err in dismissing these claims.

* * *

We have considered Plaintiff-Appellant Turret Labs' remaining arguments and find them to be without merit. Accordingly, we **AFFIRM** the judgment of the district court.

Beijing Neu Cloud Oriental Sys. Tech. Co. v. IBM

United States District Court for the Southern District of New York

March 25, 2022, Decided; March 25, 2022, Filed

21 Civ. 7589 (AKH)

Reporter

2022 U.S. Dist. LEXIS 54348 *; 2022 WL 889145

BEIJING NEU CLOUD ORIENTAL SYSTEM TECHNOLOGY CO., LTD., Plaintiff, -against- INTERNATIONAL BUSINESS MACHINES CORPORATION, et al., Defendants.

Core Terms

trade secret, misappropriation, allegations, subject matter jurisdiction, personal jurisdiction, customer information, motion to dismiss, confidential, Products, alter ego, subsidiary, fails

Counsel: [*1] For Beijing Neu Cloud Oriental System Technology Co., Ltd., Plaintiff: Clark Bakewell, Gary M. Hnath, Mayer Brown LLP, Washington, DC; Zhangyuan Ji, Chicago, IL; Bryan Nese, Mayer Brown LLP (DC), Washington, DC.

For International Business Machines Corporation, IBM World Trade Corporation, IBM China Company Limited, Defendants: Jeremy Andrew Baldoni, Quinn Emanuel Urquhart & Sullivan (NYC), New York, NY; Kevin Samuel Reed, Quinn Emanuel, New York, NY; Neil Thomas Phillips, Rachel Elizabeth Epstein, Quinn Emanuel Urquhart & Sullivan, LLP, New York, NY; Robert Francis Longtin, Quinn Emanuel Urquhart & Sullivan, New York, NY.

Judges: ALVIN K. HELLERSTEIN, United States District Judge.

Opinion by: ALVIN K. HELLERSTEIN

Opinion

POST-ARGUMENT ORDER GRANTING MOTION TO DISMISS

ALVIN K. HELLERSTEIN, U.S.D.J.:

Plaintiff initiated this action under the [federal Defend Trade Secrets Act](#), seeking to recover for alleged misappropriation that took place after Plaintiff concluded an agreement with Defendants. On March 21, 2022 I held oral argument on Defendants' motion to dismiss. For the reasons stated on the record and set forth below, Defendants' motion to dismiss is granted as to personal jurisdiction, denied as to subject matter [*2] jurisdiction, and granted for failure to state a claim. Plaintiff is given leave to replead.

BACKGROUND¹

Plaintiff is Beijing Neu Cloud Oriental System Technology Co., Ltd. ("Neu Cloud"), a Chinese company initially established by another Chinese company, TeamSun, and businessman Zhuangyan Hao. Defendants are IBM; IBM World Trade Corporation ("IBM WTC"), a wholly owned subsidiary of IBM; and

¹ The Court assumes familiarity with the factual background of this case and the parties' arguments. The following discusses only the facts necessary to resolve the pending motions.

IBM China Company Limited ("IBM China"), a wholly owned subsidiary of IBM organized under the laws of China and headquartered in China. In 2014, IBM China acquired approximately 20% of the shares in Neu Cloud.

The Complaint alleges that in 2015 Neu Cloud and IBM WTC entered an Original Equipment Manufacturer Agreement (the "OEM Agreement"). That agreement allowed Neu Cloud to purchase equipment from IBM to integrate with its own products to sell to Neu Cloud customers. Pursuant to that agreement, Neu Cloud submitted to IBM China bid requests, which included Neu Cloud's customer information. The Complaint further alleges that IBM went on to form INSPUR, a separate joint venture that now competes with Neu Cloud.

On September 10, 2021 Plaintiff initiated the instant suit alleging one count of misappropriation [*3] of trade secrets under the Defend Trade Secrets Act (DTSA). Plaintiff alleges that it shared confidential customer information with IBM China, which then used that information to form a new business venture and compete against Plaintiff. Defendants move to dismiss on subject matter jurisdiction, personal jurisdiction, and [12\(b\)\(6\)](#) grounds.

DISCUSSION

"[T]he plaintiff need persuade the court only that its factual allegations constitute a prima facie showing of jurisdiction." [Dorchester Fin. Sec., Inc. v. Banco BRJ, S.A., 722 F.3d 81, 85 \(2d Cir. 2013\)](#). "A prima facie case [of personal jurisdiction] requires non-conclusory fact-specific allegations or evidence showing that activity that constitutes the basis of jurisdiction has taken place." [Chirag v. MT Marida Marguerite Schiffahrts, 604 Fed.Appx. 16, 19](#)

[\(2d Cir. 2015\)](#). "In ruling on the motion the court may rely on facts and consider documents outside the complaint." [Cartier v. Micha, Inc., 2007 U.S. Dist. LEXIS 29785, 2007 WL 1187188, at *2 \(S.D.N.Y. Apr. 20, 2007\)](#). "Eventually, of course, the plaintiff must establish jurisdiction by a preponderance of the evidence, either at a pretrial evidentiary hearing or at trial." [Marine Midland Bank, N.A. v. Miller, 664 F.2d 899, 904 \(2d Cir. 1981\)](#).

With respect to the 12(b)(6) motion, Plaintiff's complaint "must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" [Ashcroft v. Iqbal, 556 U.S. 662, 678, 129 S. Ct. 1937, 173 L. Ed. 2d 868 \(2009\)](#) (quoting [Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570, 127 S. Ct. 1955, 167 L. Ed. 2d 929 \(2007\)](#)). A court may also consider any document relied upon by the plaintiff or which is "integral" [*4] to the complaint. See [Chambers v. Time Warner, Inc., 282 F. 3d 147, 153 \(2d Cir. 2002\)](#). For purposes of this motion, I assume all factual allegations in Plaintiff's complaint are true and draw all reasonable inferences in Plaintiff's favor. See [Khodeir v. Sayyed, 323 F.R.D. 193, 198, 200-01 \(S.D.N.Y. 2017\)](#).

1. JURISDICTION — THE 12(B)(1) AND [12\(B\)\(2\)](#) GROUNDS FOR DISMISSAL

A. Personal Jurisdiction over IBM China

Defendants argue that Plaintiff has not plead sufficient facts to establish personal jurisdiction over IBM China. The parties ardently dispute whether New York law or Chinese law should apply in assessing whether IBM China was an alter ego of IBM. Defendants argue Chinese law is narrower than New York law with respect to veil piercing. Plaintiff maintains that New York law is applicable and that, in any case, Chinese and New York law are

equivalent with respect to veil piercing. Regardless of which law applies, Plaintiff has not adequately alleged—even under New York law—that IBM China is a mere alter ego of IBM such that hailing IBM China into this court is appropriate.

In support of its claim that IBM China is the alter ego of IBM, Plaintiff alleges only that "IBM China is a 100%-owned subsidiary of [IBM] and IBM China was fully controlled by [IBM] in its interactions with Neu Cloud." Compl. ¶ 25. That is far [*5] from sufficient, even under New York law. See [Int'l Equity Invs., Inc. v. Opportunity Equity Partners, Ltd., 475 F. Supp. 2d 456, 458-59 \(S.D.N.Y. 2007\)](#) (in context of jurisdictional reverse veil piercing, a party must show "the allegedly controlled entity 'was a shell' for the allegedly controlling party"); [Am. Fuel Corp. v. Utah Energy Dev. Co., 122 F.3d 130, 134 \(2d Cir.1997\)](#). The Complaint does little more than assert the very conclusion it sets out to prove. There are no allegations that IBM China is merely a shell for IBM, only that IBM China is a subsidiary of IBM. [Marine Midland Bank, 664 F.2d at 904](#) (key question for jurisdictional veil piercing is whether the allegedly controlled entity "was a shell"); [Indem. Ins. Co. of N. Am. v. Expeditors Int'l of Washington, Inc., 382 F. Supp. 3d 302, 310 \(S.D.N.Y. 2019\)](#) (conclusory allegations that the foreign entity "[was] a wholly owned subsidiary" and was "acting as agent and on behalf of" its parent failed to establish alter ego jurisdiction). Accordingly, Defendants' motion is granted and the claim against IBM China is dismissed for lack of personal jurisdiction.

B. Subject Matter Jurisdiction

Defendant argues that the court lacks subject matter jurisdiction because Plaintiff fails to allege that its purported trade secrets are "related to" interstate or foreign commerce, as required by the DTSA. See [18 U.S.C. §](#)

[1836\(b\)\(1\)](#). The parties also dispute whether this element is jurisdictional. Regardless of whether the "related to" commerce element of the DTSA is jurisdictional, [*6] Plaintiff has done enough, at this stage, to allege that subject matter jurisdiction exists. Plaintiff alleges that its trade secrets were conveyed to Defendants as part of bid requests submitted to IBM China. Compl. ¶ 54. The trade secrets in question were lists of prospective customers for specialized products that would include IBM Power Systems, which move in commerce between the United States and China. The motion to dismiss for lack of subject matter jurisdiction is denied.

2. The [12\(b\)\(6\)](#) Grounds for Dismissal

A. The Suit is Time-Barred by the OEM Agreement

Defendants argue that the instant suit is time barred because it is covered by the OEM Agreement, which included a two-year limit for bringing claims arising from or related to the OEM Agreement. See OEM Agreement, ECF No. 25, at § 14.9. Plaintiff does not contest that the OEM Agreement can validly limit the statute of limitations, and only argues that its DTSA claim does not "arise out of" and is not "related to" the OEM Agreement. The only signatories to the OEM Agreement are Neu Cloud and IBM WTC, but as noted at oral argument, the language of the agreement sweeps broadly enough to bar suit against IBM China and IBM.

"Although the [*7] statute of limitations is ordinarily an affirmative defense that must be raised in the answer, a statute of limitations defense may be decided on a [Rule 12\(b\)\(6\)](#) motion if the defense appears on the face of the complaint." [Ellul v. Congregation of Christian Bros., 774 F.3d 791, 798 n.12 \(2d](#)

[Cir. 2014](#)). Here, the Complaint concedes that "Neu Cloud discovered this misappropriation of its trade secrets no earlier than September 26, 2018. . . . It is at this point that Neu Cloud began to suspect that its confidential customer information was being used improperly by Defendants." Compl. ¶ 74. The instant suit was not filed until September 10, 2021. Under the DTSA, the limitations begins to run from the date on which the alleged misappropriation is discovered or with reasonable diligence should have been discovered. [Zirvi v. Flatley, 433 F.Supp.3d 448, 460 \(S.D.N.Y. 2020\)](#). The statute thus began to run on the date identified in the Complaint—September 26, 2018—and the only question is whether the OEM Agreement's two-year limitations period applies to Neu Cloud's claim.

The Complaint alleges that "[u]nder the agreement with IBM, Neu Cloud submitted various bid requests to IBM China. These bid requests included customer information that was confidential to Neu Cloud and confidentially maintained by Neu Cloud as a trade secret." Compl. [*8] ¶ 54 (emphasis added). Additionally, the Complaint further alleges that "[a]s part of the agreement between the parties . . . IBM China agreed to confidentiality obligations regarding this customer information." Id. ¶ 71 (emphasis added). That language embodies the only allegations that any of the IBM corporations misappropriated Neu Cloud's trade secrets. Given that courts in this circuit have "described the term 'relating to' as equivalent to the phrases 'in connection with' and 'associated with,'" [Coregis Ins. Co. v. Am. Health Found., 241 F.3d 123, 128-29 \(2d Cir. 2001\)](#), the misappropriation alleged relates to the OEM Agreement. See also [Kortright Cap. Partners LP v. Investcorp Inv. Advisers Ltd., 327 F. Supp. 3d 673, 687 \(S.D.N.Y. 2018\)](#) (the phrase "related to" is tantamount to "having a connection, relation, or association with something"). The trade secrets in question

were allegedly disclosed to the IBM entities "under" and "as part of" the OEM Agreement. Any alleged misappropriation of those trade secrets, then, would certainly be in connection with or in relation to the OEM Agreement. The suit is thus barred by the OEM Agreement.

If Plaintiff were to prevail in its argument that IBM China is an alter ego of IBM, then all three of IBM China, IBM WTC, and IBM would be alter egos, and all would be subject to the two-year statute of limitations. Thus, [*9] if the court has personal jurisdiction and subject matter jurisdiction, the OEM time bar applies; if the time bar does not apply, then by the same token the court would lack jurisdiction.

B. Plaintiff Fails to Plead Misappropriation of a Trade Secret

The suit should be dismissed for the additional reason that Plaintiff fails to allege adequately either the existence of trade secrets, or that all of the defendants misappropriated those trade secrets. To state a claim for misappropriation under the DTSA, a party must allege that (1) it possessed a trade secret; and (2) the defendant misappropriated that trade secret. [18 U.S.C. § 1836\(b\)\(1\)](#). The DTSA defines "trade secret" broadly, to include "all forms and types of financial, business, scientific, technical, economic, or engineering information," provided that, "[1] the owner thereof has taken reasonable measures to keep such information secret; and [2] 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." [18 U.S.C. § 1839\(3\)](#).

District courts in this circuit typically require [*10] that allegations of

misappropriation plead the existence of trade secrets with sufficient specificity to inform the defendants of what they are alleged to have misappropriated. [Elsevier Inc. v. Doctor Evidence, LLC, 2018 U.S. Dist. LEXIS 10730, 2018 WL 557906, at *4 \(S.D.N.Y. Jan. 23, 2018\)](#). "[A] complaint that 'only claims general categories of information and data as trade secrets' does not state a claim under the DTSA because it 'does not adequately put [the defendant] on sufficient notice of the contours of [the] claim for misappropriation.'" [TRB Acquisitions LLC v. Yedid, 2021 U.S. Dist. LEXIS 16513, 2021 WL 293122, at *2 \(S.D.N.Y. Jan. 28, 2021\)](#) (citations omitted); see also [PaySys Int'l, Inc. v. Atos Se, 2016 U.S. Dist. LEXIS 169098, 2016 WL 7116132, at *10 \(S.D.N.Y. Dec. 5, 2016\)](#) (holding the complaint was insufficiently specific when the trade secrets were identified as "the Products, all Enhancements to the Products and all proprietary information, data, documentation and derivative works related to the Products").

Under the DTSA, misappropriation includes "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." [18 U.S.C. § 1839\(5\)](#). The term "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." [18 U.S.C. § 1839\(6\)\(A\)](#); see [Kairam v. West Side GI, LLC, 793 Fed.Appx. 23, 27-28 \(2d Cir. 2019\)](#).

1. Plaintiff does Not Adequately Plead Existence of a Trade Secret

Here, Plaintiffs have done little more than plead [*11] "broad categories of information," which is legally insufficient to state a claim. [TRB Acquisitions, 2021 U.S. Dist. LEXIS 16513, 2021 WL 293122 at, *2](#). The Complaint

alleges that "customer information" is a trade secret and asserts that such information is a trade secret by reciting the statutory elements without providing additional details. Other than noting that non-party TeamSun's efforts "helped to develop the Chinese market for IBM Power Systems products," Compl. ¶ 30, the Complaint fails to allege how Neu Cloud's trade secrets were generated and what type of information is included within the broad ambit of "customer information." Such general allegations are insufficient at this stage. See [Elsevier, 2018 U.S. Dist. LEXIS 10730, 2018 WL 557906, at *6](#) ("Alleging the existence of general categories of confidential information, without providing any details to generally define the trade secrets at issue, does not give rise to a plausible allegation of a trade secret's existence."); [Universal Processing LLC v. Weile Zhuang, 2018 U.S. Dist. LEXIS 168730, 2018 WL 4684115, at *3 \(S.D.N.Y. Sept. 28, 2018\)](#).

Furthermore, because Plaintiff has not "identified anything about the process of developing [customer] lists" or "shown how their particular value derives from their secrecy," it fails to state a claim. [Democratic Nat'l Comm. v. Russian Fed'n, 392 F. Supp. 3d 410, 448 \(S.D.N.Y. 2019\)](#) (citing [Council on Am.-Islamic Relations Action Network, Inc. v. Gaubatz, 82 F. Supp. 3d 344, 361 \(D.D.C. 2015\)](#)).

2. Plaintiff Does Not Plead Misappropriation as to IBM WTC

Plaintiff must plead facts that explain how each defendant [*12] misappropriated trade secrets. See [Xavian Ins. Co. v. Marsh & McLennan Companies, Inc., 2019 U.S. Dist. LEXIS 65067, 2019 WL 1620754, at *6 \(S.D.N.Y. Apr. 16, 2019\)](#). It has not done so with respect to IBM WTC. The Complaint makes no allegations specific to IBM WTC's

misappropriation of trade secrets. Plaintiff argues only that all IBM defendants benefitted from INSPUR's use of the trade secrets, but that is far from enough to find that IBM WTC misappropriated any trade secret.

3. Plaintiff Does Not Plead a Territorial Link to IBM China

The DTSA requires that to proceed against a foreign defendant, a Plaintiff must plead that "an act in furtherance of the offense was committed in the United States." [18 U.S.C. § 1837](#). Nowhere does the Complaint detail any act that occurred in the United States in furtherance of the misappropriation of trade secrets. In its brief, Plaintiff argues that general Internet use in the context of emails between Neu Cloud and IBM China suffice. Even assuming that an act as generic as sending an email via the Internet could satisfy the requirements of the DTSA, both Neu Cloud and IBM China are Chinese companies located in China, and there is nothing to suggest that a discrete act in furtherance of the misappropriation took place in the United States. Accordingly, the claim against IBM China fails for this [*13] reason as well.

CONCLUSION

The motion to dismiss for lack of personal jurisdiction is granted as to defendant IBM China and the motion to dismiss for failure to state a claim is granted as to all defendants. The motion to dismiss for lack of subject matter jurisdiction is denied. Plaintiff may file an Amended Complaint, if it can, to cure the defects discussed in this opinion by April 11, 2022. Defendants shall move or answer by May 9, 2022.

The initial case management conference will be held June 17, 2022 at 10:00 a.m. The Clerk shall terminate ECF No. 19.

SO ORDERED.

Dated: March 25, 2022

New York, New York

/s/ Alvin K. Hellerstein

ALVIN K. HELLERSTEIN

United States District Judge

End of Document



Neutral

As of: November 2, 2022 2:15 AM Z

[Kinship Partners, Inc. v. Embark Veterinary, Inc.](#)

United States District Court for the District of Oregon

January 3, 2022, Decided; January 3, 2022, Filed

No. 3:21-cv-01631-HZ

Reporter

2022 U.S. Dist. LEXIS 2804 *; 2022 WL 72123

KINSHIP PARTNERS, INC., Plaintiff, v.
EMBARK VETERINARY, INC. and ROBIN P.
SMITH, Defendants.

Core Terms

trade secret, misappropriation, documents, downloaded, confidential, resignation, inevitable disclosure doctrine, preliminary injunction, disclose, Drive, proprietary information, alleges, non competition agreement, former employee, competitor, disclosure, confidential information, injunction, discovery, employees, accessed, files, plaintiff's claim, merits, brand, injunctive relief, irreparable harm, no evidence, courts, public interest

Counsel: [*1] For Plaintiff: Kjersten H. Turpen, K&L Gates LLP, Portland, OR; Jonathan Stoler, Adam Pekor, Lindsay C. Stone, Sheppard, Mullin, Richter & Hampton LLP, New York, NY,.

For Defendants: Peter Hawkes, Edward A. Piper, Angeli Law Group LLC, Portland, OR; Jeffrey M. Edelson, Markowitz Herbold PC, Portland, OR.

Judges: MARCO A. HERNÁNDEZ, United States District Judge.

Opinion by: MARCO A. HERNÁNDEZ

Opinion

OPINION & ORDER

HERNÁNDEZ, District Judge:

Plaintiff Kinship Partners, Inc. ("Kinship") seeks an injunction that prohibits Defendants Robin P. Smith ("Smith") and Embark Veterinary, Inc. ("Embark") "from possessing, using, disclosing, or benefitting from . . . Kinship's trade secrets and confidential and proprietary information in any manner." Pl. Mot. 1, ECF 2. Plaintiff also seeks to enjoin Smith from working for Embark for a period of 12 months. *Id.* Smith, who previously worked at Kinship, resigned from his position on November 1, 2021 and had intended to begin employment with Embark on November 15, 2021. Ex. 2; Smith Decl. ¶ 16. The Court issued a Temporary Restraining Order ("TRO") on November 10, 2021 and held an evidentiary hearing on Plaintiff's Motion for a Preliminary Injunction on November 22, 2021. For the reasons [*2] stated below, the Court denies Plaintiff's motion and dissolves the TRO.

BACKGROUND

Kinship and Embark, as the two leading providers of canine DNA testing services worldwide, are head-to-head competitors. Compl. ¶ 2, ECF 1. Defendant Smith is the former Head of Product for Kinship's Wisdom brand, which offers customers pet DNA testing and related services. Ex. 6; Compl. ¶ 17. Smith was hired by Kinship on December 17, 2020

"to lead all aspects of the product development, user experience, and visual design of Wisdom, as well as to devise and lead the brand's overall business strategy. Yoo Decl. ¶ 11, ECF 2-1. Smith had previously worked for Kinship's parent company, Mars Petcare, US ("Mars") beginning July 2019. Compl. ¶ 3. Smith was an "at-will" employee at Kinship, which means either Smith or Kinship could terminate the employment relationship at any time. Ex. 6, ¶ 7. Kinship requests, but does not require, that employees give two weeks' notice upon resignation. Ex. 24D.

On December 17, 2020, when he was hired to his recent position at Kinship, Smith signed a Proprietary Information and Inventions Agreement ("IP Agreement") and a Confidential Information and Invention Assignment Agreement. [*3] ("Confidentiality Agreement"). Yoo Decl. ¶ 15; Ex. 24C. Paragraph 5(a) of the IP Agreement and paragraph 2(a) of the Confidentiality Agreement contain identical language as follows:

Confidential Information. (a) Protection of Information. I agree, at all times during the term of the [employment] Relationship and thereafter, to hold in strictest confidence, and not to use, except for the benefit of the Company to the extent necessary to perform my obligations to the Company under the Relationship, and not to disclose to any person, firm, corporation or other entity, without written authorization from the Company in each instance, any Confidential Information (as defined below) that I obtain, access or create during the term of the Relationship, whether or not during working hours, until such Confidential Information becomes publicly and widely known and made generally available through no wrongful act of mine or of others who were under confidentiality obligations as to the item or items involved. I further agree not to make copies of such

Confidential Information except as authorized by the Company.

Ex. 24C. Paragraph 4 of the Confidentiality Agreement states in part:

I agree that, at [*4] the time of termination of the [employment] Relationship, I will deliver to the Company (and will not keep in my possession, recreate or deliver to anyone else) any and all devices, records, data, notes, reports, proposals, lists, correspondence, specifications, drawings, blueprints, sketches, laboratory notebooks, materials, flow charts, equipment, other documents or property, or reproductions of any of the aforementioned items developed by me pursuant to the Relationship or otherwise belonging to the Company, its successors or assigns.

Id. Smith also signed and received a copy of Kinship's Associate Handbook, which notifies employees that they must "keep all such confidential and proprietary information in confidence." Ex. 24D. All Kinship employees sign an IP Agreement, a Confidentiality Agreement, and the Associate Handbook. Some high-level Kinship employees are also required to sign noncompetition agreements as a condition of employment. Smith was not asked and did not sign a noncompetition agreement when he was first hired by Mars in July 2019 or when was hired by Kinship in December 2020. Smith Decl. ¶ 5.

On October 1, 2021, Embark CEO Ryan Boyko sent Smith a message through LinkedIn, [*5] inviting him to discuss the possibility of employment at Embark. *Id.* at ¶ 1. Smith claims that he was initially not interested because he did not want to work for Kinship's competitor. *Id.* at ¶ 3. But Smith became interested in the opportunity when he learned that Embark planned to move in a different direction than Kinship. *Id.* Embark specifically wanted "to get more into research and

potentially drug discovery." *Id.* On October 15, after a series of scheduling emails, Smith met with Boyko over video chat. *Id.* at ¶ 5. Over the next two weeks, Smith met with several other Embark representatives to discuss the possibility of employment. *Id.* Smith accepted an offer of employment with Embark on October 29 and signed a formal offer letter on October 31. *Id.* at ¶ 6; Ex. 2. Embark's onboarding document for Smith states: "you will focus on supporting and improving the Research & Development arm of Embark (internally called "Branch 2")[,] . . . your work will *not* be focused on our existing product's strategy, sales or NPS. Success in your role will be measured on the rate and value of new discovery[.]" Ex. 42.

In the months leading up to his resignation from Kinship, Smith continued his work [*6] as Head of Product for the Wisdom brand. In September 2021, Smith gave a presentation to Kinship's most senior executives entitled "Wisdom **2022+** Product & Innovation" that described the strategic vision for the Wisdom brand. Compl. ¶40. On October 27, 2021, Smith again presented the Wisdom brand's product roadmap and strategic vision to Kinship's senior directors. *Id.* at 41.

On November 1, 2021, Smith, who was working remotely from home, sent a Letter of Resignation by email to three senior leaders at Kinship, indicating that his last day would be November 12, 2021, and that he intended to join Embark in a role focusing on "research and discovery." Yoo Decl. ¶¶58, 61; Ex. 19. In his resignation email, Smith stated:

I also plan to cease business activity today until directed on how you'd like to proceed — please advise. The only company property in my possession is the laptop I've been using over the past few years. I'm happy to bring this into the office or mail as directed.

Ex. 19. Within two hours of the resignation email, Smith received a call from Luis Alvarado, Kinship's head of human relations, who told Smith that Kinship was "accelerating" his resignation to be effective immediately. [*7] Smith Decl. ¶ 9. Kinship did not conduct an exit interview with Smith. *Id.* at ¶10.

On the day of Smith's resignation, Kinship conducted a "forensic review of his network activity." Compl. ¶ 43; Yoo Decl. ¶ 68. The forensic review found that Smith downloaded 27 documents—such as google presentations, PDFs, and excel files—from Kinship's secure cloud-based computer drive ("Shared Drive") during the six-month period before his resignation. Ex. 21. The last download was on October 1, 2021. *Id.*

Kinship also created a log of all files held in Kinship's Shared Drive that Smith accessed between August 1, 2021 and November 1, 2021. Ex. 26. On the morning of November 1, 2021, before he sent his notice of resignation, Smith accessed and either reviewed or edited files stored on the Shared Drive seven times. Five times, he accessed a file called "Wisdom Panel Business Meeting Notes," which is a "living document" on which Smith provided updates each week to senior leaders of the Wisdom brand. Ex. 26. Smith states that on the morning he resigned, he entered his weekly updates into the Wisdom Panel Business Meeting Notes document so that the information would not be lost. Smith Decl. ¶ 7.

On November [*8] 4, 2021, Kinship sent a courier to Smith's home to retrieve his company laptop computer. Kinship solicited an outside firm to conduct a forensic review of that device. Def. Ex. 22; Compl. ¶ 43. The forensic review of Smith's laptop computer was not completed at the time of the preliminary injunction hearing.

STANDARDS

A preliminary injunction is an "extraordinary remedy that may only be awarded upon a clear showing that the plaintiff is entitled to such relief." [*Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 22, 129 S. Ct. 365, 172 L. Ed. 2d 249 \(2008\)](#). A plaintiff seeking a preliminary injunction must show (1) that he or she is likely to succeed on the merits; (2) he or she is likely to suffer irreparable harm in the absence of preliminary relief; (3) the balance of the equities tips in his or her favor; and (4) an injunction is in the public interest. [*Id.* at 20](#).

In the Ninth Circuit, courts may apply an alternative "serious questions" test, which allows for a preliminary injunction when a plaintiff shows that "serious questions going to the merits" were raised and the balance of hardships tips sharply in plaintiff's favor, assuming the other two elements of the [*Winter*](#) test are met. [*All. for the Wild Rockies v. Cottrell*, 632 F.3d 1127, 1131-32 \(9th Cir. 2011\)](#). This formulation applies a sliding scale approach where a stronger showing of one element may offset a weaker [*9] showing in another element. [*Id.* at 1131](#). Nevertheless, the party requesting a preliminary injunction must carry its burden of persuasion by a "clear showing" of the four elements set forth above. [*Lopez v. Brewer*, 680 F.3d 1068, 1072 \(9th Cir. 2012\)](#).

DISCUSSION

Plaintiff brings claims and seeks a preliminary injunction against Defendants Smith and Embark under the [*Defend Trade Secrets Act \("DTSA"\)*, 18 U.S.C. § 1836](#), and the [*Oregon Uniform Trade Secrets Act \("OUTSA"\)*, Or. Rev. Stat. § \("O.R.S."\) 646.461 et seq.](#) Under the DTSA, a court may grant injunctive relief "to prevent any actual or threatened misappropriation . . . on such terms as the

court deems reasonable." [*18 U.S.C. § 1836\(b\)\(3\)\(A\)\(i\)*](#). The OUTSA authorizes courts to temporarily, preliminarily, or permanently enjoin actions that result in actual or threatened misappropriation of proprietary trade secrets. [*O.R.S. 646.463\(1\)*](#).

Plaintiff claims that Defendants Smith and Embark have engaged in both actual and threatened misappropriation of Plaintiff's trade secrets. Compl. ¶¶ 73, 88. Plaintiff bases its claims on two theories: (1) Smith has actually misappropriated its trade secrets and (2) Defendants threaten misappropriation of Plaintiff's trade secrets because Smith "will inevitably use and disclose them in connection with his duties at Embark." Pl. Mot. 19-20.

Plaintiff [*10] notes that Smith had access to Kinship's confidential and proprietary trade secrets, accessed and downloaded documents containing confidential and proprietary information while employed at Kinship, and then abruptly resigned with the intent to work for Embark—Kinship's primary competitor. Plaintiff alleges that Smith's downloading of documents containing confidential information is "suspicious," and thus Plaintiff believes that "Smith has shared or intends to share the information contained in these documents with Embark in connection with his employment." *Id.* at 19. Plaintiff also claims that Smith will be unable to fulfill his job responsibilities at Embark "without disclosing or using Kinship's trade secrets and confidential and proprietary information." Compl. ¶¶ 72, 87.

Plaintiff seeks a preliminary injunction that: "(1) prohibits Defendants from possessing, using, disclosing, or benefitting from, either directly or indirectly, Kinship's trade secrets and confidential and proprietary information; and (2) prohibits Smith from working for Embark for a period of at least 12 months from the date he resigned from Kinship." Pl. Mot. 1.

I. Likelihood of Success on the Merits

A. Actual Misappropriation [*11]

To succeed on its claim that Defendants actually misappropriated Plaintiff's trade secrets, Plaintiff must show (1) the information was in fact a trade secret; (2) Plaintiff took reasonable measures to maintain the secrecy of information; and (3) Defendants' conduct constitutes misappropriation. [Univ. Acct. Serv., LLC v. Schulton, No. 3:18-CV-1486-SI, 2019 U.S. Dist. LEXIS 96710, 2019 WL 2425122, at *5 \(D. Or. June 10, 2019\)](#). The OUTSA provides a broad definition of "trade secret," which includes any information such as "cost data, customer list, formula, pattern, compilation, program, device, method, technique or process" that derives actual or potential "independent economic value" from not being generally known to the public. [O.R.S. 646.461\(4\)](#). Under the DTSA, "the term 'trade secret' means all forms and types of financial, business, scientific, technical, economic, or engineering information." [18 U.S.C. § 1839\(3\)](#). Plaintiff alleges the trade secrets in Smith's possession include all aspects of Wisdom's brands strategic plan to compete with Embark. Pl. Mot. 10. Defendants do not contest that the subject of Plaintiff's concern and allegations are trade secrets. The Court agrees.

The Court also finds that Plaintiff took reasonable measures to protect its trade secrets. Every Kinship employee, [*12] including Smith, signs an IP Agreement and a Confidentiality Agreement, which specifically prohibit employees from disclosing confidential or proprietary information to anyone outside the company. Kinship employees use a secure shared cloud-based computer drive to maintain company work product. The Confidentiality Agreement and the Associate Handbook specify that upon termination of

employment, each employee must return all company equipment and all documents containing proprietary information. These measures demonstrate that Plaintiff intended and took steps to keep confidential certain documents and information about its competitive strategy against Embark to which Smith had access.

Next, Plaintiff must provide evidence that Smith misappropriated Plaintiff's trade secrets. Both the DTSA and the OUTSA define "misappropriation" as the acquisition of a trade secret "by a person who knows or has reason to know that the trade secret was acquired by improper means" or the "disclosure or use of a trade secret of another without express or implied consent[.]" [18 U.S.C. § 1839\(5\)\(A\)-\(B\)](#); [O.R.S. 646.461\(2\)](#). "Improper means" includes theft, bribery, misrepresentation, and breach of a duty to maintain secrecy. [18 U.S.C. § 1839\(6\)\(A\)](#); [O.R.S. 646.461\(1\)](#). A plaintiff bears the [*13] burden of proving misappropriation and, at minimum, must show the defendant acted with some degree of bad faith. [Ferring B.V. v. Allergan, Inc., 4 F. Supp. 3d 612, 628 \(S.D.N.Y. 2014\)](#). The plaintiff must "specifically connect allegations of misappropriation to specific [d]efendants' actions." [Physician's Surrogacy, Inc. v. German, No. 17cv718-MMA \(WVG\), 2018 U.S. Dist. LEXIS 16261, 2018 WL 638229, at *8 \(S.D. Cal. Jan. 31, 2018\)](#).

i. Downloaded Documents

Plaintiff alleges that "in the weeks leading up to his resignation, [Smith] surreptitiously downloaded nearly 30 confidential business documents, including presentation materials outlining Wisdom's product roadmap for the next five years from the Company's Shared Drive." Yoo Decl. ¶ 68. Kinship's forensic review shows that Smith downloaded 27 documents over a six-month period. The documents include "an analysis of the competitive pressures Kinship is facing from

Embark" and "Kinship's internal product development timeline to beat Embark to the market." Pl. Mot. 19. Plaintiff alleges that Smith's downloads are "suspicious" and that Smith intends to share the information contained in those documents with Embark because "there is no other reason for Smith to have downloaded this information on the eve of his resignation." *Id.*

Plaintiff is correct that an employee who, without authorization, procures their employer's trade secrets and confidential [*14] information immediately before terminating employment may have engaged in misappropriation. See [A Place for Mom v. Perkins, 475 F. Supp. 3d 1217, 1227 \(W.D. Wash. 2020\)](#) (holding that the defendant employee misappropriated the plaintiff employer's protectible trade secrets when she emailed documents and reports to herself prior to resigning). But Plaintiff presents no evidence that Smith acted in bad faith, engaged in nefarious activity, or used improper means to acquire its trade secrets.

First, Kinship does not have a stated company policy against downloading documents from the company's shared drives. In fact, both Yoo and Timothy Hirsch, Kinship's head of legal compliance, testified that they occasionally download company documents to their personal devices. Although Plaintiff claims the frequency with which Smith downloaded documents is suspicious, it does not specify how many downloads by an employee over a given period of time is considered unusual. Plaintiff also provides no evidence that Smith tried to hide the fact that he downloaded documents from the Shared Drive. No one at Kinship told Smith not to download documents, and he was never reprimanded for doing so while he was employed at Kinship.

Second, Plaintiff cannot show that Smith's downloading [*15] of documents lacked a

business purpose. See [CleanFish, LLC v. Sims, No. 19-cv-03663-HSG, 2020 U.S. Dist. LEXIS 46191, 2020 WL 1274991, at *10 \(N.D. Cal. Mar. 17, 2020\)](#) (holding that, to state a claim for misappropriation, a plaintiff must allege facts that "tend to exclude an innocent explanation") (internal quotation and citation omitted). Plaintiff presents no evidence that Smith downloaded files for reasons other than for the performance of his job. Despite Plaintiff's claim that Smith downloaded confidential documents "in the weeks leading up to his resignation," Smith did not download any documents after he started discussing employment with Embark. Smith last downloaded a document from Kinship's Shared Drive on October 1, 2021—one month before he resigned.¹ The Court finds no indication that Smith's downloads were anything but innocuous.

Third, Plaintiff provides no evidence that Smith retained the documents he downloaded. In fact, Plaintiff concedes that it has no first-hand knowledge of Smith retaining any of Kinship's confidential documents. Yoo Dep. 160:2-5; 170:5-22. Nor can Plaintiff show that Smith has shared information contained in the documents he downloaded with Embark employees or anyone else outside of Kinship. Thus, Plaintiff fails to provide factual [*16] support for its allegation that Smith's downloaded documents from Kinship's Share Drive for nefarious reasons.

ii. *Files Accessed*

Plaintiff alleges Smith misappropriated its trade secrets by logging onto Kinship's Shared Drive and reviewing several confidential documents "as recently as an hour before he tendered his resignation." Compl. ¶ 45. But Plaintiff admits that it does not know why Smith accessed the files. Plaintiff cannot show

¹ Smith was first contacted by Embark on October 1, 2021 and did not respond to Embark's request until October 8, 2021.

that Smith accessed the files for reasons other than to perform his job duties at Kinship. Smith states that all the files he accessed are ones he used on regular basis during the course of his employment. Smith "edited" the "Wisdom Panel Business Meeting Notes" file less than an hour before his resignation. Ex. 26. But Smith explains that he updated the file because doing so was his ongoing job responsibility, and he wanted to make sure the information did not get lost.

In summary, Smith had legitimate, innocuous reasons to download and access confidential files while he was employed at Kinship. Because Plaintiff fails to show Smith's actions were improper, it is unlikely to succeed on the merits of its claim that Defendants actually misappropriated Kinship's [*17] trade secrets.

B. Threatened Misappropriation: The Inevitable Disclosure Doctrine

Plaintiff claims that Smith's employment with Embark threatens the misappropriation of Kinship's trade secrets and its confidential and proprietary information. Plaintiff asserts that because of Smith's key role in developing Kinship's strategy to compete against Embark, his decision to "assume a nearly identical role at Embark will inevitably lead him to use and disclose Kinship's trade secrets[.]" Pl. Mot. 20. According to Plaintiff, even if Smith did not improperly access or obtain any confidential documents, he retains knowledge of Kinship's trade secrets in his head and cannot work for Embark without using or disclosing those secrets in the normal course of his employment.² In seeking relief without

evidence of actual misappropriation, Plaintiff urges the Court to adopt and apply the doctrine of inevitable disclosure. *Id.*

The seminal case that recognized the inevitable disclosure doctrine as a viable theory for trade secret misappropriation is [PepsiCo, Inc. v. Redmond, 54 F.3d 1262 \(7th Cir. 1995\)](#). The rationale underlying the inevitable disclosure doctrine is that a plaintiff may establish threatened misappropriation simply by the fact that the "defendant's [*18] new employment will inevitably lead that defendant to rely on plaintiff's trade secrets." [Phoseon Tech., Inc. v. Heathcote, No. 3:19-cv-2018-SI, 2019 U.S. Dist. LEXIS 221633, 2019 WL 72497, at *8-9](#). In [PepsiCo](#), the Seventh Circuit held that the inevitability that a former employee would rely on the plaintiff's trade secrets in his new job with plaintiff's direct competitor demonstrated a likelihood of success on plaintiff's trade secret misappropriation claim under the [Illinois Trade Secrets Act \("ITSA"\)](#). [54 F.3d at 1271](#). In other words, a former employee threatens misappropriation of trade secrets simply by holding knowledge of those secrets in their head while working for a direct competitor. The remedy for threatened misappropriation under this theory is to enjoin the former employee from working for the competitor. See [Payment All. Int'l, Inc. v. Ferreira, 530 F. Supp. 2d 477, 482-83 \(S.D.N.Y. 2007\)](#) (enjoining a former employee from working for a competitor under the inevitable disclosure doctrine based on his knowledge of former employer's customers and marketing strategy because "he may unintentionally transmit information gain through his association with [his former employer]").

i. Application of the Inevitable Disclosure Doctrine to the DTSA and OUTSA

The inevitable disclosure doctrine constitutes a narrow avenue for courts to provide injunctive

²"In effect, Smith helped write Wisdom's entire playbook, and he retains that playbook to this day. If he joins Embark or any other direct competitor, he will inevitably draw on Wisdom's 'plays' to give Embark an unfair competitive edge in a battle for market share in the highly competitive pet care marketplace." Yoo Decl. ¶ 57.

relief for threatened misappropriation [*19] of trade secrets. The doctrine requires a court to recognize and enforce a de facto noncompetition agreement to which the former employee is bound, even where no express agreement exists. See [Bayer Corp. v. Roche Molecular Sys., Inc.](#), 72 F. Supp. 2d 1111, 1120 (N.D. Cal. 1999) ("To the extent that the theory of inevitable disclosure creates a de facto covenant not to compete without a nontrivial showing of actual or threatened use or disclosure, it is inconsistent with California law."). Pursuant to federal law, the DTSA specifically forecloses courts from granting relief based on the inevitable disclosure doctrine because such relief restrains employment. Under the DTSA, "a court may grant an injunction to prevent any actual or threatened misappropriation . . . provided the order does not prevent a person from entering into an employment relationship[.]" [18 U.S.C. § 1836\(b\)\(3\)\(A\)\(i\)\(I\)](#) (emphasis added). Based on the plain language of the statute, the DTSA provides no avenue for the Court to grant Plaintiff its requested relief.

Several states recognize the inevitable disclosure doctrine under their respective trade secret misappropriation statutes. See [Phoseon Tech.](#), 2019 U.S. Dist. LEXIS 221633, 2019 WL 7282497, at *11 ("Seventeen states appear to have adopted the inevitable disclosure doctrine in one form or another.").³ Oregon is not one of those states. In [Phoseon](#), [*20] this Court declined to decide whether the plaintiff's claim of threatened misappropriation based on the inevitable discovery doctrine was likely to succeed. *Id.* The former employee in that case was subject

to a noncompetition agreement, and the Court granted injunctive relief on that basis alone. *Id.* But, in dictum, the Court noted that it was unlikely that Oregon would adopt the inevitable disclosure doctrine because of the state legislature's recent trend of allowing greater freedom of employment. *Id.* ("If one evaluates the likelihood of the Oregon Supreme Court adopting the inevitable disclosure doctrine by considering the history of legislation over the years, the result does not yield confidence that the doctrine will be adopted in Oregon anytime soon.").

The Oregon legislature limited the enforceability of noncompetition agreements in 2007 and has evinced a clear concern for the rights of its employees. 2007 Or. Laws 2765. Among other limitations, current Oregon law makes noncompetition agreements voidable unless the employer informed the employee in writing at least two weeks before the start of employment that a noncompetition is required as a condition of employment. [O.R.S. 653.295\(1\)\(a\)\(A\)](#). Oregon employment [*21] law does not explicitly prohibit protecting trade secrets through injunctive relief that restricts employment. See [O.R.S. 653.295\(5\)](#) ("Nothing in this section restricts the right of any person to protect trade secrets or other proprietary information by injunction or any other lawful means under other applicable laws."). But because Oregon limits and makes voidable even express noncompetition agreements, the Court finds that Oregon courts would be unlikely to interpret the OUTSA as providing an avenue for de facto, post-hoc noncompetition agreements as would be required by the inevitable disclosure doctrine. See [IKON Off. Sols., Inc. v. Am. Off. Prods., Inc.](#), 178 F. Supp. 2d 1154, 1168 (D. Or. 2001) (rejecting a plaintiff's trade secrets claim in part because granting relief would amount to "a long-term non-competition requirement, but without any of the restrictions that the Oregon legislature has imposed upon non-competition

³ California, Colorado, Louisiana, Maryland, and Virginia have specifically rejected the doctrine. [Phoseon Tech.](#), 2019 U.S. Dist. LEXIS 221633, 2019 WL 7282497, at *11; see, e.g., [Bayer Corp.](#), 72 F. Supp. 2d at 1120. ("California trade secrets law does not recognize the theory of inevitable disclosure; indeed, such a rule would run counter to the strong public policy in California favoring employee mobility.").

agreements"). Because Oregon law favors employee mobility, the Court declines to adopt the inevitable disclosure doctrine or apply it to this case.

ii. *Plaintiff's Claims under the Inevitable Disclosure Doctrine*

Even if the Court were to recognize the inevitable disclosure doctrine, Plaintiff cannot show a likelihood of success on the merits based on this theory. [*22] Under the inevitable disclosure doctrine, Plaintiff must show that Smith would need to use or disclose his knowledge of Kinship's trade secrets to perform his job at Embark. See [Amazon.com, Inc. v. Powers, No. C12-1911RAJ, 2012 U.S. Dist. LEXIS 182831, 2012 WL 6726538, at *7 \(W.D. Wash. Dec. 27, 2012\)](#) ("Evidence of what [the former employee] knows is not enough; [plaintiff] must show that [the former employee] is likely to disclose it."). In addition, a plaintiff must show that a former employee takes to the competitor more than just general knowledge and skills acquired during their employment. [PepsiCo, 54 F.3d at 1269](#).

"The crux of an inevitable disclosure argument in this context is a showing that an employee's new job so closely resembles her old one that it would be impossible to work in that job without disclosing confidential information." [Amazon.com, 2012 U.S. Dist. LEXIS 182831, 2012 WL 6726538, at *7](#); see [Lam Rsch. Corp. v. Deshmukh, No. C04-5435FDB, 2005 U.S. Dist. LEXIS 54389, 2005 WL 8173156, at *5 \(W.D. Wash. Jan. 3, 2005\)](#) (holding that a plaintiff could only proceed on an inevitable discovery claim by showing it was impossible for the defendant in his new role "to make management decisions without benefitting from the intimate knowledge of [plaintiff's] trade secrets, business plans, and strategies to which [d]efendant was privy"). To show that disclosure is inevitable, a plaintiff must "make a detailed showing of a similarity between an

employee's new job and old job." [Amazon.com, 2012 U.S. Dist. LEXIS 182831, 2012 WL 6726538, at *7](#).

Plaintiff alleges, but cannot [*23] demonstrate, that Smith's role at Embark is substantially similar to his prior role at Kinship. Smith testified that he only became interested in Embark's offer to discuss employment when he learned that Embark was planning to move in a different direction, which would provide him the opportunity to work in a different role. Emily Levada, Chief Product Officer and Smith's new direct supervisor at Embark, testified that Smith will work in a section of Embark that focuses on new product discovery and early development. He was not hired to work in the section of Embark that competes with Kinship in marketing and selling dog DNA products. While Smith admits that his new job will involve some product development, his focus will be on research and discovery. Embark's onboarding document for Smith describes a role focused more on scientific research and discovery than on marketing and business strategy.⁴ Thus, Plaintiff cannot meet its burden of showing that Smith will work in a substantially similar role at Embark as his prior position at Kinship.

Next, Plaintiff presents no facts that show Smith would necessarily disclose Kinship's trade secrets to fulfill his job duties at Embark. Nothing [*24] in Plaintiff's presented evidence suggests that Smith intends to disclose Kinship's trade secrets to his new employer. Smith acted with candor when he resigned from Kinship. Cf. [PepsiCo, 54 F.3d at 1271](#) (finding that the defendant's lack of candor in pursuing and accepting a job with a competitor

⁴ Embark's onboarding document for Smith states, "you will focus on supporting and improving the Research & Development arm of Embark (internally called "Branch 2")[.] . . . your work will *not* be focused on our existing product's strategy, sales or NPS. Success in your role will be measured on the rate and value of new discovery[.]" Ex. 42.

to be a factor in determining whether he would threaten misappropriation of the plaintiff's trade secrets). Smith's supervisor at Embark presented strategies she would employ to ensure that Smith does not work on projects that would require him to use his specific knowledge Kinship's trade secrets. The Court finds that such measures are sufficient to protect against inevitable disclosure. Thus, even if the Court were to apply the inevitable disclosure doctrine, Plaintiff cannot show that Smith's position at Embark would require him to disclose or use Kinship's trade secrets. Plaintiff's allegations of threatened disclosure are no more than speculation.

Because Plaintiff does not present sufficient facts demonstrating actual misappropriation and cannot rely on the inevitable disclosure doctrine for threatened misappropriation, it does not meet its burden of showing a substantial likelihood of success on the merits. [*25]

II. Irreparable Harm

Plaintiff alleges that it will be "substantially and irreparably harmed if Smith is allowed to join or continue working for Embark, as he will necessarily use and disclose Kinship's trade secrets in connection with his employment there." Pl. Mot. 25. Plaintiff is correct that "the misappropriation of trade secrets constitutes *prima facie* evidence of irreparable harm." [Phoseon Tech., 2019 U.S. Dist. LEXIS 221633, 2019 WL 7282497, at *12](#). "A trade secret once lost is, of course, lost forever." [FMC Corp. v. Taiwan Tainan Giant Indus. Co., Ltd., 730 F.2d 61, 63](#). Injunctive relief is the appropriate remedy for the harm caused by trade secret misappropriation because the loss typically cannot be measured in money damages. *Id.*

But Plaintiff cannot show irreparable harm because there is no evidence that Smith acted

in bad faith or has breached his Confidentiality Agreement with Kinship. Plaintiff presents no evidence that Smith inappropriately procured or retained any confidential or proprietary documents. Plaintiff claims that without an injunction preventing Smith from working for Embark, "Smith's decisions will inevitably be informed by his detailed knowledge of Kinship's strategic plans for gaining a competitive advantage against Embark." Pl. Mot. 26. Thus, in alleging irreparable harm, Plaintiff relies [*26] on the inevitable disclosure doctrine—a legal theory that is unavailable. As the Court cannot grant relief based on the inevitable disclosure doctrine, Plaintiff does not meet its burden of showing it will suffer irreparable harm if a preliminary injunction is not granted.

III. Balance of the Equities

In evaluating whether to grant a preliminary injunction, courts "must balance the competing claims of injury and must consider the effect on each party of the granting or withholding of the request relief." [Winter, 555 U.S. at 24](#). For a court to grant injunctive relief, "the injunction must do more good than harm (which is to say the balance of equities favors the plaintiff)." [Alliance for the Wild Rockies, 632 F.3d at 1133](#) (quoting [Hoosier Energy Rural Elec. Co-op., Inc. v. John Hancock Life Ins. Co., 582 F.3d 721, 725 \(7th Cir. 2009\)](#)). Under the Ninth Circuit's "serious questions" test, a weak showing of likelihood of success may be enough to justify a preliminary injunction if serious questions going to the merits were raised. *Id.* But in that situation, the plaintiff must show that "the balance of hardships tips sharply in the plaintiff's favor." [Lands Council v. McNair, 537 F.3d 981, 987 \(9th Cir. 2008\)](#) (en banc) (internal quotation and citation omitted).

Here, Plaintiff seeks to enjoin Smith from

working for Embark for a period of 12 months. Plaintiff has a strong interest in protecting its trade secrets. But [*27] Plaintiff cannot show its trade secrets are under threat of misappropriation because it relies on a legal theory that is unavailable in Oregon. Defendants, on the other hand, have an interest in the free flow of commerce and of employment. A preliminary injunction would restrain Smith's freedom to be employed where he chooses. Given Oregon's proclivity to protect the rights of workers to choose where they are employed, and the Court's reluctance to create a de facto noncompetition agreement where none exists, the Court finds the balance of equities favors Defendants and weighs against a preliminary injunction.

IV. Public Interest

"In exercising their sound discretion, courts of equity should pay particular regard for the public consequences in employing the extraordinary remedy of injunction." [Winter, 555 U.S. at 24](#) (quoting [Weinberger v. Romero-Barcelo, 456 U.S. 305, 312, 102 S. Ct. 1798, 72 L. Ed. 2d 91 \(1982\)](#)). "When the reach of an injunction is narrow, limited only to the parties, and has no impact on non-parties, the public interest will be at most a neutral factor in the preliminary injunction analysis." [Stormans v. Selecky, 586 F.3d 1109, 1138-39 \(9th Cir. 2009\)](#).

Plaintiff asserts that the public interest factor weighs in its favor because, if Smith works for and discloses trade secrets to Embark, such action would have public consequences by [*28] "unfairly stifl[ing] competition in an extremely limited market." Pl. Mot. 28. But Plaintiff provides little support for this claim. If Smith were to disclose Kinship's trade secrets in the course of his new employment, Embark could potentially gain an advantage over Kinship. But Plaintiff fails to show how that

advantage would stifle competition in the industry as a whole. Thus, any potential anticompetitive impact of Defendants' alleged misappropriation is too speculative to be considered a factor in the public interest analysis.

In contrast, given the Oregon legislature's demonstrated intent to protect employee mobility, restricting employment through a preliminary injunction could undermine Oregon's public interest goals. Accordingly, the public interest factor is at best neutral, but may weigh slightly against granting a preliminary injunction.

CONCLUSION

Because Plaintiff has not met its burden of persuasion as to the four [Winter](#) elements, the Court dissolves the Temporary Restraining Order [13] and DENIES Plaintiff's Motion for a Preliminary Injunction [2].

IT IS SO ORDERED.

DATED: **January 3, 2022**

/s/ Marco A. Hernández

MARCO A. HERNÁNDEZ

United States District Judge



Positive

As of: November 2, 2022 2:18 AM Z

[Idexx Lab'ys v. Bilbrough](#)

United States District Court for the District of Maine

August 2, 2022, Decided; August 2, 2022, Filed

2:22-cv-00056-JDL

Reporter

2022 U.S. Dist. LEXIS 136676 *; 2022 WL 3042966

IDEXX LABORATORIES, INC., Plaintiff v.
GRAHAM BILBROUGH, Defendant

Subsequent History: Adopted by, Dismissed by [Idexx Lab'ys v. Graham Bilbrough, 2022 U.S. Dist. LEXIS 181179 \(D. Me., Oct. 4, 2022\)](#)

Prior History: [Idexx Lab'ys, Inc. v. Bilbrough, 2022 U.S. Dist. LEXIS 82982, 2022 WL 1451525 \(D. Me., May 9, 2022\)](#)

Core Terms

trade secret, misappropriation, Products, inevitable disclosure doctrine, veterinary, Fecal, confidential, diagnostic, injunction, tests, trade secret information, motion to dismiss, offerings, Clinical, Antigen, plans, research and development, veterinarians, disclosing, disclosure, sector

Counsel: [*1] For IDEXX LABORATORIES INC, Plaintiff: ERIC M. FERRANTE, LEAD ATTORNEY, PRO HAC VICE, NIXON PEABODY LLP, ROCHESTER, NY; RICHARD H. TILGHMAN, IV, LEAD ATTORNEY, PRO HAC VICE, NIXON PEABODY LLP, CHICAGO, IL; ROBERT C. BROOKS, LEAD ATTORNEY, VERRILL DANA LLP, PORTLAND, ME; STEPHEN J. JONES, LEAD ATTORNEY, NIXON PEABODY LLP, ROCHESTER, NY; ELIZABETH TULL JOHNSTON, VERRILL DANA LLP, PORTLAND, ME.

For GRAHAM BILBROUGH, MELISSA LAPOINTE, Defendants: MATTHEW D. MORGAN, MCKEE LAW LLC PA, AUGUSTA, ME; WALTER F. MCKEE, MCKEE LAW LLC PA, AUGUSTA, ME.

Judges: John C. Nivison, United States Magistrate Judge.

Opinion by: John C. Nivison

Opinion

RECOMMENDED DECISION ON DEFENDANT'S MOTION TO DISMISS

Plaintiff alleges that Defendant, a former employee, will necessarily misappropriate its trade secrets in his current employment in violation of the federal Defend Trade Secrets Act and the Maine Uniform Trade Secrets Act. (Complaint, ECF No. 1.) Plaintiff seeks to enjoin Defendant from disclosing Plaintiff's trade secrets and from working on product offerings to which the trade secret information would be relevant.

Defendant has moved to dismiss Plaintiff's complaint.¹ (Motion, ECF No. 29.) Defendant

¹Plaintiff originally asserted claims against Defendants Graham Bilbrough, and Melissa LaPointe. Both defendants filed the present motion. Plaintiff voluntarily dismissed its claims against Ms. LaPointe. (Notice of Voluntary Dismissal Without Prejudice, ECF No. 33.) This recommended decision

contends Plaintiff has failed to assert [*2] an actionable federal claim, and, therefore, dismissal of Plaintiff's complaint, including Plaintiff's state law claims, is warranted.

Following a review of the parties' submissions I recommend the Court grant the motion to dismiss.

FACTUAL AND PROCEDURAL BACKGROUND

The following facts are drawn from Plaintiff's complaint. A plaintiff's factual allegations are generally deemed true when evaluating a motion to dismiss. See [McKee v. Cosby](#), 874 F.3d 54, 59 (1st Cir. 2017) (considering a motion to dismiss pursuant to [Rule 12\(b\)\(6\)](#)); [Merlonghi v. United States](#), 620 F.3d 50, 54 (1st Cir. 2010) (considering a motion to dismiss pursuant to [Rule 12\(b\)\(1\)](#)).

Plaintiff develops, manufactures, and distributes products and services for the companion animal veterinary, livestock and poultry, water testing, and dairy sectors. (Complaint ¶ 9.) Defendant worked for Plaintiff in various high-level roles from October 2006 until his resignation on January 27, 2022. (*Id.* ¶ 16.) For most of his employment with Plaintiff, Defendant worked within IDEXX's Companion Animal Group Medical Organization. Most recently, Defendant held the title of Associate Director, Global Medical Strategy and Innovation and reported directly to Plaintiff's Vice President and Chief Medical Officer. (*Id.* ¶ 18.) From January through September 2021, Defendant worked [*3] as the Director Associate Fellow, in Plaintiff's Corporate Strategy Group. (*Id.* ¶ 19.)

Among Plaintiff's products in the veterinary diagnostic sector are its fecal antigen tests (the "IDEXX Antigen Products") and fecal PCR tests (the "IDEXX PCR Products"), which tests

assist veterinarians in the detection of fecal parasites in a stool sample (collectively, the "IDEXX Fecal Solutions"). (*Id.* ¶ 14.) Another product in the veterinary diagnostic sector is its point-of-care hematology test, which allows veterinarians to perform in-office blood tests without the need for an outside lab. (*Id.* ¶ 15.)

During his employment with Plaintiff, Defendant acquired knowledge of Plaintiff's proprietary and trade secret information, including but not limited to Plaintiff's strategic business assessments, prioritization planning, and its research and development portfolio and product roadmap for a variety of Plaintiff's current and future product offerings. (*Id.* ¶ 20.) Defendant worked with Plaintiff's research and development team, including in the analysis of the marketability of various product lines and in the development of veterinary products, including the IDEXX Fecal Solutions. (*Id.* ¶ 21.)

In his [*4] work, Defendant acquired knowledge of confidential product testing results concerning the IDEXX Antigen Products and Plaintiff's efforts to improve the IDEXX Antigen Products, including the efforts to expand the number and type of parasites identified by the IDEXX Antigen Products and to develop new ways for veterinarians to run antigen tests. (*Id.* ¶ 22.) Plaintiff considers its product development plans and internal data regarding its IDEXX Fecal Solutions to be trade secrets (the "IDEXX Fecal Solutions Trade Secrets"). (*Id.*)

Defendant was also involved in the development of Plaintiff's Clinical Decision Support ("CDS") project that explores cutting-edge ways to use data analytics to help veterinarians interpret symptoms and test results to make better clinical decisions. (*Id.* ¶ 23.) Plaintiff considers its product development plans and internal data in Clinical Decision Support to be trade secrets (the "CDS Trade Secrets"). (*Id.*) In his 2021 self-evaluation,

Defendant described his role in CDS's strategic direction and development: "I have helped build the vision for Clinical Decision Support ['CDS']. (*Id.* ¶ 24.) Rather than a collection of 'interpretation tools,' I have shown the [*5] path to a reimagination of how veterinarians consume diagnostic information and respond. (*Id.*) In CDS, I was integral to the project that 'painted the picture' and lead to [Plaintiff]'s first significant financial investment... For much of 2021, I was the *de facto* Clinical Product Manager." (*Id.*)

Defendant was also involved in a confidential project for Plaintiff to develop the next generation of veterinary diagnostic tests by identifying gaps and opportunities in the veterinary sector (the "Unmet Needs Project"). (*Id.* ¶ 25.) Through the Unmet Needs Project, Defendant had access to Plaintiff's confidential and proprietary marketing and clinical information gathered to validate Plaintiff's potential strategic priorities, which Plaintiff considers trade secrets (the "Unmet Needs Data Trade Secrets"). (*Id.*) Defendant also had access to Plaintiff's trade secrets relating to Plaintiff's chemistry development plans for point-of-care diagnostic tests (the "Chemistry Trade Secrets"). (*Id.* ¶ 26.) In addition, Defendant was involved in the research and development of Plaintiff's oncology product offerings and in developing Plaintiff's product plans in veterinary oncology. (*Id.* ¶ 27.) Plaintiff [*6] considers its research and development activities and plans for future product offerings in veterinary oncology to be trade secrets (the "Oncology Strategy Trade Secrets"). (*Id.*)

Plaintiff has implemented measures designed to maintain its trade secrets as confidential, including marking sensitive documents as "confidential," limiting access to trade secrets to employees who have a need to know the trade secret information, maintaining computer security features and devices to prevent

external access to trade secrets, requiring employees to acknowledge a Code of Ethics that requires Plaintiff's confidential information be kept confidential, reminding personnel about the importance of maintaining confidences, and requiring employees to sign agreements that prohibit the disclosure of trade secret information. (*Id.* ¶ 12.) Plaintiff's Code of Ethics requires that employees "[s]afeguard confidential information from public disclosure." (*Id.* ¶ 13.)

Defendant resigned from Plaintiff effective January 27, 2022. (*Id.* ¶ 28.) Despite requests from his former colleagues and supervisors, Defendant refused to disclose the identity of his new employer. (*Id.* ¶ 29.) Plaintiff subsequently learned that [*7] Defendant is now working for Antech Diagnostics ("Antech"), one of Plaintiff's principal competitors. (*Id.* ¶ 30.) Among other products, Antech offers a fecal PCR test (the "Antech PCR Products") that competes directly with the IDEXX Fecal Solutions in the veterinary diagnostic sector. (*Id.* ¶ 31.) On January 31, 2022, four days after his resignation from Plaintiff, Defendant represented Antech on an American Association of Veterinary Parasitologists Hookworm Taskforce call on which the Antech PCR Products were presented. (*Id.* ¶ 32.)

Plaintiff contends Defendant is working for Antech in a role that is substantively identical to his role at Plaintiff, which role involves the clinical development and strategic planning for Antech diagnostic products, including the Antech PCR Products. (*Id.* ¶ 33.) Plaintiff alleges that given the direct competition between the IDEXX Fecal Solutions and the Antech PCR Products, Defendant could not work on the Antech PCR Products without disclosing and/or using Plaintiff's trade secrets. (*Id.* ¶ 34.) Defendant's knowledge of the IDEXX Antigen Products, Plaintiff asserts, would be invaluable to Antech as it would

allow Antech to focus its research and development [*8] efforts on areas where it can better compete with Plaintiff. (*Id.*)

Plaintiff alleges that in his current employment, Defendant will necessarily misappropriate Plaintiff's trade secrets in violation of the federal [Defend Trade Secrets Act \(DTSA\), 18 U.S.C. §§ 1836 et seq.](#), and the [Maine Uniform Trade Secrets Act \(MUSTA\), 10 M.R.S. §§ 1541 et seq.](#) Plaintiff seeks injunctive relief prohibiting Defendant from (1) directly or indirectly disclosing or using Plaintiff's trade secret information in his employment with Antech; and (2) directly or indirectly working on Antech product offerings that are competitive with Plaintiff's products "from which [Defendant] derived [Plaintiff's] trade secrets." (*Id.* PageID #16, ¶¶ A(i)-(ii).)

LEGAL STANDARD

Defendant argues Plaintiff has failed to allege a federal cause of action. Pursuant to [Federal Rule of Civil Procedure 12\(b\)\(6\)](#), a party may move to dismiss a claim for "failure to state a claim upon which relief can be granted." In reviewing a motion to dismiss under [Rule 12\(b\)\(6\)](#), a court "must evaluate whether the complaint adequately pleads facts that 'state a claim to relief that is plausible on its face.'" [Guilfoile v. Shields, 913 F.3d 178, 186 \(1st Cir. 2019\)](#) (quoting [Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570, 127 S. Ct. 1955, 167 L. Ed. 2d 929 \(2007\)](#)). In doing so, a court "assume[s] the truth of all well-pleaded facts and give[s] the plaintiff the benefit of all reasonable inferences therefrom." *Id.* (quoting [Thomas v. Rhode Island, 542 F.3d 944, 948 \(1st Cir. 2008\)](#)). Defendant also argues that if the Court determines [*9] that Plaintiff has not asserted a federal claim, the Court would lack jurisdiction over Plaintiff's state law claim.

DISCUSSION

A. Plaintiff's Misappropriation Claim Under DTSA

Congress enacted DTSA in 2016 "as a needed update to Federal law" and to "provide a single, national standard for trade secret misappropriation with clear rules and predictability for everyone involved." H.R. Rep. [No. 114-529](#), at 200 (2016). Congress noted that "[w]hile 48 states have adopted variations of the [Uniform Trade Secret Act], the state laws vary in a **number** of ways and contain built-in limitations that make them not wholly effective in a national and global economy." H.R. Rep. [No. 114-529](#), at 198. Although "Congress went out of its way to make clear that the DTSA does not preempt state trade secret laws' but 'merely provides a complementary Federal remedy[,]' that "does not mean that the statutes are the *same*." [Advantage Payroll Servs., Inc. v. Rode, No. 2:21-cv-00020-NT, 2021 WL 5999187, at *5 \(D. Me. Dec. 20, 2021\)](#) (quoting [Brand Energy & Infrstr. Servs., Inc. v. Irex Contracting Grp., Civil Action No. 16-2499, 2017 WL 1105648, at *7 n.17 \(E.D. Pa. Feb. 24, 2017\)](#) (emphasis in original).

DTSA defines "misappropriation," in part, as the "disclosure or use of a trade secret of another without express or implied consent by a person who ... at the time of disclosure or use, knew or had reason [*10] to know that the knowledge of the trade secret was ... acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret" [18 U.S.C. § 1839\(5\)\(B\)\(ii\)\(II\)](#).

To "prevail on a claim of misappropriation of trade secrets, a plaintiff must show 1) the information is a trade secret; 2) the plaintiff took reasonable steps to preserve the secrecy of the information; and 3) the defendant used improper means, in breach of a confidential

relationship, to acquire and use the trade secret." [*Incase Inc. v. Timex Corp.*, 488 F.3d 46, 52 \(1st Cir. 2007\)](#).

For purposes of his motion to dismiss, Defendant does not contest that the identified information to which he was privy as an employee of Plaintiff was trade secret information, nor does he argue that Plaintiff failed to take reasonable steps to conserve its secrecy. Defendant focuses on the third element of a misappropriation claim, arguing Plaintiff has not sufficiently alleged an actionable "use" of Plaintiff's trade secrets.

Plaintiff has not alleged that Defendant has in fact disclosed or used Plaintiff's trade secret information. Plaintiff instead asserts Defendant inevitably will disclose its trade secrets during his employment with Antech. Plaintiff thus seeks to [*11] proceed based on the inevitable disclosure doctrine. Pursuant to the inevitable disclosure doctrine, "a plaintiff may prove a claim of trade secret misappropriation by demonstrating that defendant's new employment will inevitably lead him [or her] to rely on the plaintiff's trade secrets." [*PepsiCo, Inc. v. Redmond*, 54 F.3d 1262, 1269 \(7th Cir. 1995\)](#). In other words,

a former employee threatens misappropriation of trade secrets simply by holding knowledge of those secrets in their head while working for a direct competitor.... The inevitable disclosure doctrine constitutes a narrow avenue for courts to provide injunctive relief for threatened misappropriation of trade secrets. The doctrine requires a court to recognize and enforce a de facto noncompetition agreement to which the former employee is bound, even where no express agreement exists.

[*Kinship Partners, Inc. v. Embark Veterinary, Inc.*, No. 3:21-cv-01631-HZ, 2022 WL 72123,](#)

[at *6-7 \(D. Or. Jan. 3, 2022\)](#).²¹

Defendant contends that the inevitable disclosure doctrine cannot sustain Plaintiff's claim for injunctive relief under DTSA. Under DTSA, a court may grant an injunction "to prevent any actual or threatened misappropriation," provided the order does not "prevent a person from entering into an employment relationship, and that the conditions placed on such employment shall be based on evidence of threatened [*12] misappropriation and not merely on the information the person knows." [18 U.S.C. § 1836\(b\)\(3\)\(A\)\(ii\)\(I\)](#). Defendant maintains that Plaintiff has alleged no actual threat of misappropriation. Rather, Defendant argues, Plaintiff's claim is based on the information Defendant knows and Plaintiff's concern that Defendant will disclose the information.

One court recently observed that "there is no judicial consensus on whether DTSA permits application of the inevitable disclosure doctrine." [*Sunbelt Rentals, Inc. v. McAndrews*, 552 F. Supp. 3d 319, 331 \(D. Conn. 2021\)](#). The lack of consensus appears to be the product of courts assessing the doctrine without distinguishing between recovery under DTSA or a similar, but not identical, state trade secrets act. See, e.g., [*Fres-co Sys. USA, Inc. v. Hawkins*, 690 Fed. App'x 72, 76 \(3d Cir. 2017\)](#) (applying DTSA and Pennsylvania Uniform Trade Secret Act); [*Molon Motor & Coil Corp. v. Nidec Motor Corp.*, No. 16 C 03545, 2017 WL 1954531, *5-7 \(N.D. Ill. May 11, 2017\)](#) (applying DTSA and Illinois Trade Secrets Act); [*UCAR Tech. \(USA\) Inc. v. Li*, No. 5:17-cv-01704-EJD, 2017 U.S. Dist. LEXIS 206816, 2017 WL 6405620, at *3 \(N.D. Cal.](#)

²One court has explained, "an alternative reading of the inevitable disclosure doctrine is that it is just one way of showing a threatened disclosure." [*Barilla Am., Inc. v. Wright*, No. 4-02-CV-90267, 2002 U.S. Dist. LEXIS 12773, 2002 WL 31165069, *9 \(S.D. Iowa July 5, 2002\)](#).

[Dec. 15, 2017](#)) (applying DTSA and California Uniform Trade Secrets Act). However, "[t]here are key differences between the DTSA's language and the language of other trade secret statutes." [Brand Energy & Infrstr. Servs., Inc. v. Irex Contracting Grp., Civil Action No. 16.2499, 2017 WL 1105648, at *3 \(E.D. Pa. Feb. 24, 2017\)](#). Most courts in which the doctrine has been applied to DTSA claims have not directly addressed the DTSA requirement that an injunction must be "based on evidence of threatened misappropriation and not merely on the information the person knows." [18 U.S.C. § 1836\(b\)\(3\)\(A\)\(ii\)\(I\)](#).

When the court [*13] in [Kinship Partners](#) assessed the language when considering the question of whether the inevitable disclosure doctrine applies to DTSA claims, the court concluded that "DTSA specifically forecloses courts from granting relief based on the inevitable disclosure doctrine *because* such relief restrains employment. ... Based on the plain language of the statute, the DTSA provides no avenue for the Court to grant Plaintiff its requested relief." [Kinship Partners, 2022 WL 72123, at *7](#) (emphasis in original).

As reflected by the court's analysis in [Kinship Partners](#), resolution of the question begins with consideration of the language of DTSA. That is, when interpreting a statutory provision, a court begins "where all such inquiries must begin: with the language of the statute itself." [Republic of Sudan v. Harrison, 139 S. Ct. 1048, 1056, 203 L. Ed. 2d 433 \(2019\)](#) (internal quotation marks and citations omitted). A court "accord[s] the statutory text its ordinary meaning by reference to the specific context in which the language is used, and the broader context of the statute as a whole." [Recovery Grp., Inc. v. Cmm'r of Internal Revenue, 652 F.3d 122, 125 \(1st Cir. 2011\)](#) (internal quotation marks and citations omitted). The plain language of [section 1836\(b\)\(3\)\(A\)\(ii\)\(I\)](#) states that an injunction, the only relief Plaintiff

seeks, may not issue "to prevent a person from entering into an employment relationship" based "merely on the information the person [*14] knows." Because the inevitable disclosure doctrine permits relief without any proof of actual or an identified threat of disclosure under the theory that a person with certain information will necessarily use the information at some point in his or her new employment, the doctrine allows relief based "merely on the information the person knows." The plain language of the statute, therefore, forecloses application of the inevitable disclosure doctrine to Plaintiff's DTSA-based claim requesting that the Court enjoin Plaintiff from working on Antech product offerings that are competitive with Plaintiff's products.

To the extent there is an ambiguity in the statute, a review of the development of the statute suggests Congress did not intend the doctrine to apply to DTSA claims. An earlier version of the draft legislation provided that an injunction could issue "to prevent any actual or threatened misappropriation ... provided the order does not prevent a person from accepting an offer of employment under conditions that avoid actual or threatened misappropriation." S. 1890, [§ 2](#) (proposed for codification at [18 U.S.C. § 1836\(b\)\(3\)](#)). Congress received some comments critical of the language. See, e.g., Eric Goldman, [*15] et al, *Professors' Letter in Opposition to the Defend Trade Secrets Act of 2015*, at 5³ (arguing that this language "could reasonably be interpreted to endorse the inevitable disclosure doctrine as a matter of federal law"). Congress subsequently revised the language to its present form, suggesting that Congress did not intend for the inevitable disclosure doctrine to apply.⁴

³ Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2699760.

⁴ As explained in this Court's order on Plaintiff's motion for

In sum, based on the plain language of the statute, the inevitable disclosure doctrine does not apply to claims brought pursuant to DTSA. Because Plaintiff seeks to enjoin Defendant from working for Antech in the capacity for which he was hired based on the inevitable disclosure doctrine, Plaintiff has not alleged an actionable claim under DTSA.

B. Plaintiff's Misappropriation Claim Under State Law

Plaintiff has also asserted a claim under the Maine trade secrets statute, MUSTA, which claim Plaintiff asserted in this Court based on the Court's supplemental jurisdiction.⁵ The Court's assessment of Plaintiff's claim under DTSA does not govern Plaintiff's MUSTA claim. Congress noted that "if a State's trade secrets law authorizes additional remedies, those State-law remedies will still be available." S. Rep. 114-2. Thus, "a [*16] state that has adopted the inevitable disclosure

expedited discovery, "at least one scholar has observed that the inevitable disclosure doctrine might have informed the DTSA requirement that an injunction must be based on threatened misappropriation and not merely on the information a person knows. See M. Claire Flowers, Facing the Inevitable: The Inevitable Disclosure Doctrine and the Defend Trade Secrets Act of 2016, 75 Wash. & Lee L. Rev. 2207, 2230-31 (2018) (arguing that the legislative history and plain language "indicate that Congress did not intend for courts to apply inevitable disclosure in DTSA claims")." (Order on Motion for Discovery at 6, ECF No. 30.)

⁵ Title 28 U.S.C. § 1367, which governs the Court's exercise of its supplemental jurisdiction, provides:

[I]n any civil action of which the district courts have original jurisdiction, the district courts shall have supplemental [*17] jurisdiction over all other claims that are so related to claims in the action within such original jurisdiction that they form part of the same case or controversy under Article III of the United States Constitution. Such supplemental jurisdiction shall include claims that involve the joinder or intervention of additional parties.

28 U.S.C. § 1367(a).

doctrine can still afford injunctive relief under that doctrine for a misappropriation claim brought under state law." 1 Roger Milgrim & Eric Bensen, *Milgrim on Trade Secrets* § 5.02 (2021). Whether a plaintiff could proceed on a claim under MUSTA based on the inevitable disclosure doctrine is apparently an open question under Maine law. The issue is most appropriately decided in state court. Where Plaintiff has not alleged a claim under federal law, the Court should decline supplemental jurisdiction over Plaintiff's claim under MUSTA. 28 U.S.C. 1367(c)(1) (proper to decline jurisdiction where "the claim raises a novel or complex issue of State law."); 28 U.S.C. § 1367(c)(3) ("The district court may decline to exercise supplemental jurisdiction over a claim ... if ... the district court has dismissed all claims over which it has original jurisdiction."); see Rodríguez v. Doral Mort. Corp., 57 F.3d 1168, 1177 (1st Cir. 1995) ("As a general principle, the unfavorable disposition of a plaintiff's federal claims at the early stages of a suit ... will trigger the dismissal without prejudice of any supplemental state law claims.").

CONCLUSION

Based on the foregoing analysis, I recommend the Court grant Defendant's motion to dismiss and dismiss Plaintiff's complaint.

NOTICE

A party may file objections to those specified portions of a magistrate judge's report or proposed findings or recommended decisions entered pursuant to 28 U.S.C. § 636(b)(1)(B) for which de novo review by the district court is sought, together with a supporting memorandum, within fourteen (14) days of being served with a copy thereof. A responsive memorandum shall be filed within fourteen


(14) days after the filing of the objection.
Failure to file a timely objection shall constitute a waiver of the right to de novo review by the district court and to appeal the district court's order.

/s/ John C. Nivison

U.S. Magistrate Judge

Dated this **2nd** day of **August, 2022**.

End of Document

 An official website of the United States government
[Here's how you know](#)



Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Monday, May 9, 2022

Chemist Sentenced for Stealing Trade Secrets, Economic Espionage and Wire Fraud

A federal judge in Greeneville, Tennessee, sentenced a Michigan woman today to 168 months, the equivalent of 14 years, in prison for a scheme to steal trade secrets, engage in economic espionage and commit fraud. The defendant was also ordered to serve three years of supervised release and pay a \$200,000 fine.

In April 2021, following a 13-day jury trial, Xiaorong You, aka Shannon You, 59, of Lansing, Michigan, was convicted of conspiracy to commit trade secret theft, conspiracy to commit economic espionage, possession of stolen trade secrets, economic espionage and wire fraud.

"As the evidence at trial showed, the defendant stole valuable trade secrets and intended to use them to benefit not only a foreign company, but also the government of China," said Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division. "Today's sentence reflects the seriousness of this offense, as well as the Department of Justice's commitment to protect our nation's security by investigating and prosecuting those who steal U.S. companies' intellectual property."

"When companies invest huge amounts of time and money to develop world-class technologies, only to have those technologies stolen, the results are devastating," said Assistant Attorney General Kenneth A. Polite Jr. of the Justice Department's Criminal Division. "Here, the defendant intended not only to enrich herself and her China-based partners, but also the government of China. Crimes like the defendant's threaten both victim companies and the economic security of the nation as a whole. This case should serve as a warning to those entrusted with valuable trade secrets: if you break the law, you will be punished."

"Stealing trade secrets of U.S. companies for the benefit of the Chinese government will be vigorously prosecuted in the Eastern District of Tennessee, and today's 14-year sentence reflects the seriousness of this defendant's crimes," said U.S. Attorney Francis M. Hamilton III for the Eastern District of Tennessee. "The corporate vigilance and subsequent cooperation with federal law enforcement that brought this defendant to justice is to be commended; our national security depends on it."

"Stealing technology isn't just a crime against a company," said Acting Assistant Director Bradley S. Benavides of the FBI's Counterintelligence Division. "It's a crime against American workers whose jobs and livelihoods are impacted. Today's sentencing is a reminder that the FBI and its partners will hold accountable those who break our laws and threaten our economic and national security."

"Ingenuity, innovation, and perseverance are the time-honored trademarks of American business and entrepreneurship," said Special Agent in Charge Joseph E. Carrico of the FBI's Knoxville Field Office. "In the current global state of commerce, corporations are forced to place an increased emphasis on the protection of trade secrets and intellectual property. The FBI will not sit by while any nation-state attempts to steal or incentivizes the theft of trade secrets from successful corporations. The FBI is committed to working with industry to hold those accountable who would attempt to steal technology or trade secrets at the cost of American businesses, their employees, and their livelihood."

According to court documents and evidence presented at trial, You stole valuable trade secrets related to formulations for bisphenol-A-free (BPA-free) coatings for the inside of beverage cans. You were granted access to the trade secrets while working at The Coca-Cola Company in Atlanta, and Eastman Chemical Company in Kingsport, Tennessee. The stolen trade secrets belonged to major chemical and coating companies including Akzo-Nobel, BASF, Dow Chemical, PPG, Toychem, Sherwin Williams and Eastman Chemical Company, and cost nearly \$120 million to develop.

You stole the trade secrets to set up a new BPA-free coating company in China. You and her Chinese corporate partner, Weihai Jinhong Group, received millions of dollars in Chinese government grants to support the new company (including a Thousand Talents Plan award). Your Thousand Talents Program application and other evidence presented at trial showed that she intended to benefit not only Weihai Jinhong Group, but also the governments of China, the Chinese province of Shandong, the Chinese city of Weihai and the Chinese Communist Party.

Until recently, BPA was used to coat the inside of cans and other food and beverage containers to help minimize flavor loss and prevent the container from corroding or reacting with the food or beverage contained therein. However, due to BPA's potential health risks, companies began searching for BPA-free alternatives. Developing these BPA-free alternatives was a very expensive and time-consuming process.

From December 2012 through August 2017, You were employed as Principal Engineer for Global Research at Coca-Cola, which had agreements with numerous companies to conduct research and development, testing, analysis and review of various BPA-free technologies. Because of Your extensive education and experience with BPA and BPA-free coating technologies, she was one of a limited number of Coca-Cola employees with access to BPA-free trade secrets belonging to Akzo-Nobel, BASF, Dow Chemical, PPG, Toychem and Sherwin Williams. From approximately September 2017 through June 2018, You were employed as a packaging application development manager for Eastman Chemical Company in Kingsport, Tennessee, where she was one of a limited number of employees with access to trade secrets belonging to Eastman.

The FBI's Knoxville Field Office and HSI investigated the case.

Assistant U.S. Attorney Mac D. Heavener III for the Eastern District of Tennessee; Senior Counsel Matt Walczewski of the Criminal Division's Computer Crime and Intellectual Property Section; and Trial Attorney Nic Hunter of the National Security Division's Counterintelligence and Export Control Section are prosecuting the case. Valuable assistance was provided by Assistant U.S. Attorney T.J. Harker for the Eastern District of Tennessee.

Topic(s):

Financial Fraud
Intellectual Property
Counterintelligence
National Security

Component(s):

Criminal Division
Criminal - Computer Crime and Intellectual Property Section
Federal Bureau of Investigation (FBI)
National Security Division (NSD)
USAO - Tennessee, Eastern

Press Release Number:

22-487

Updated May 10, 2022

FILED

FEB 12 2019

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT GREENEVILLE

Clerk, U. S. District Court
Eastern District of Tennessee
At Greeneville

UNITED STATES OF AMERICA)
)
 v.)
)
 XIAORONG YOU)
 aka SHANNON YOU)
 and)
 LIU XIANGCHEN)

No. 2:19-CR-14
Judge: Greer

FILED UNDER SEAL

INDICTMENT

The Grand Jury in and for the Eastern District of Tennessee, sitting in Greeneville, charges:

COUNT ONE

(Conspiracy to Commit Theft of Trade Secrets, 18 U.S.C. § 1832(a)(5))

1. Beginning not later than on or about March 16, 2017 and continuing through at least on or about November 10, 2018, in the Eastern District of Tennessee and elsewhere, the defendants XIAORONG YOU and LIU XIANGCHEN, knowingly conspired and agreed together and with "Co-Conspirator #1" and other persons known and unknown to the grand jury, to steal trade secret information that cost at least approximately \$119,600,000 to develop, that is:

(a) With intent to convert a trade secret that was related to a product and service used in and intended for use in interstate and foreign commerce, to the economic benefit of persons other than the trade secret's owner, and intending and knowing that the offense would injure the trade secret's owner, the defendants conspired to knowingly steal, and without authorization appropriate, take, carry away, and conceal such information, in violation of 18 U.S.C. § 1832(a)(1);

(b) With intent to convert a trade secret that was related to a product and service used in and intended for use in interstate and foreign commerce, to the economic benefit of persons other than the trade secret's owner, and intending and knowing that the offense would injure the trade secret's owner, the defendants conspired to knowingly and without authorization copy, duplicate, photograph, download, upload, replicate, transmit, deliver, send, mail, communicate, and convey such information, in violation of 18 U.S.C. § 1832(a)(2); and

(c) With intent to convert a trade secret that was related to a product and service used in and intended for use in interstate and foreign commerce, to the economic benefit of persons other than the trade secret's owner, and intending and knowing that the offense would injure the trade secret's owner, the defendants conspired to knowingly possess such information, knowing the same to have been stolen and appropriated, obtained, and converted without authorization, in violation of 18 U.S.C. § 1832(a)(3);

such trade secret information ("TSI") relating primarily to:

- a formulation for a bisphenol-A-free (as defined in paragraph 2) coating for use inside cans (*e.g.*, beer or other beverage cans) that prevents the contents of the can from interacting with the metal surface of the can over time, owned by "TSI Owner #1";
- the chemical substances used to create a substitute for epoxy coatings containing bisphenol-A, owned by "TSI Owner #2";
- newly-developed bisphenol-A-free polyolefin dispersion coatings for the inside of food and drink cans, such as aluminum soda cans, that protect both the can from corrosion and its contents from contamination by the can's material, owned by "TSI Owner #3";
- formulas used to develop bisphenol-A-free interior sprays for aluminum and steel food and beverage cans, owned by "TSI Owner #4";

- the development of bisphenol-A-free liquid coating compositions for forming FDA-compliant and EU-compliant, food-contact-safe coatings on the surfaces of metal beverage cans and in the development of analogous coatings for metal food cans owned by “TSI Owner #5”;
 - information used in the process of developing “Gen-2,” bisphenol-A-free coating technologies for aluminum food-grade beverage containers, owned by “TSI Owner #6”;
- and
- resins for use in bisphenol-A-free coatings for the interior of rigid metal packaging, owned by “Employer #2” located in Kingsport, Tennessee.

BACKGROUND

2. Corporations like “Employer #1” use various chemical technologies to coat the inside of cans and other food and beverage containers. These chemical technologies were designed to adhere to the container, minimize flavor loss, and prevent the container from corroding or reacting with the food or beverage contained therein, all without posing any threat to human health. Until recently, many containers were coated using a polycarbonate plastic made from a chemical called bisphenol-A (“BPA”). Due to possible harmful effects of BPA, companies like Employer #1 began searching for alternatives to BPA; such alternatives are known as “bisphenol-A not intended” or “BPA-NI” (“BPA-free”). These alternatives are difficult to develop.

3. During the time period of the conspiracy, Employer #1 had agreements with numerous companies including TSI Owner #1, TSI Owner #2, TSI Owner #3, TSI Owner #4, TSI Owner #5, and TSI Owner #6, to conduct research and development, testing, analysis, and review of various BPA-free-related technologies.

4. These agreements contemplated that TSI Owner #1, TSI Owner #2, TSI Owner #3, TSI Owner #4, TSI Owner #5, and TSI Owner #6 would each disclose confidential information, including TSI, to Employer #1 for the narrow purpose of performing such research and development, testing, analysis, and review. These agreements also required that Employer #1 would take reasonable measures to protect the confidentiality of TSI, including by requiring that TSI be further disclosed only on a need-to-know basis and only to persons specifically approved by the owners of the TSI.

5. XIAORONG YOU had extensive education and experience with BPA and BPA-free coating technologies. XIAORONG YOU claimed a Ph.D. in Polymer Science and Engineering from Lehigh University and worked in various sophisticated roles for numerous companies throughout the United States dating back to May 1992. XIAORONG YOU had particular experience developing coating technologies for various food and beverage manufacturers.

6. From in or about December 2012 through on or about August 31, 2017, XIAORONG YOU was employed as Principal Engineer for Global Research at Employer #1 in Atlanta, Georgia. During her employment at Employer #1, XIAORONG YOU was one of a limited number of employees with access to TSI belonging to TSI Owner #1, TSI Owner #2, TSI Owner #3, TSI Owner #4, TSI Owner #5, and TSI Owner #6, pursuant to the agreements discussed above.

7. Employer #2, located in Kingsport, TN, also competes in the BPA-free coating technologies business.

8. From on or about September 1, 2017 through on or about June 22, 2018, XIAORONG YOU was employed as a Packaging Application Development Manager for

Employer #2 in Kingsport, Tennessee. During her employment at Employer #2, XIAORONG YOU was one of a limited number of employees with access to TSI belonging to Employer #2.

9. During the conspiracy, "China Company #1" was a company based in the Shandong province of China. During the conspiracy, LIU XIANGCHEN was the General Manager of China Company #1.

10. The Chinese government sponsored a program entitled "The Thousand Talents." This program was designed to induce individuals with advanced technical education, training, and experience residing in Western countries to return or move to China and use their expertise to promote China's economic and technological development. The Thousand Talents application process was competitive, and those who were selected sometimes received an annual payment from the Chinese government calculated as a percentage of the applicant's current salary.

11. Various provincial Chinese governments had award programs similar to the national Thousand Talent Program. The provincial government for Shandong Province sponsored a program entitled "Yishi-Yiyi." Like the Thousand Talents Program, Yishi-Yiyi paid a monetary award to successful applicants with proposals to bring technology to the province.

12. "Co-Conspirator #1" is believed to be a relative of XIAORONG YOU, and is believed to live in China.

OBJECTS OF THE CONSPIRACY

13. It was part of the conspiracy that XIAORONG YOU, LIU XIANGCHEN, and Co-Conspirator #1, acting together, conspired to steal, appropriate, copy, duplicate, photograph, download, upload, replicate, transmit, deliver, send, communicate, convey, receive, and possess TSI related to a product or service used or intended for use in interstate or foreign commerce, for the economic benefit of persons other than the owners of the TSI, intending or knowing that the

offense would injure TSI Owner #1, TSI Owner #2, TSI Owner #3, TSI Owner #4, TSI Owner #5, TSI Owner #6, and Employer #2.

MANNER AND MEANS

It was part of the conspiracy that XIAORONG YOU, LIU XIANGCHEN, and Co-Conspirator #1 formulated a plan and agreement that, among other things, included the following:

14. XIAORONG YOU, LIU XIANGCHEN, and Co-Conspirator #1 agreed that XIAORONG YOU would exploit her employment with Employer #1 and Employer #2 to steal TSI belonging to TSI Owner #1, TSI Owner #2, TSI Owner #3, TSI Owner #4, TSI Owner #5, TSI Owner #6, and Employer #2.

15. XIAORONG YOU, LIU XIANGCHEN, and Co-Conspirator #1 agreed that XIAORONG YOU would then transfer the stolen TSI to China Company #1 and that XIAORONG YOU would become an employee of China Company #1.

16. In exchange, LIU XIANGCHEN agreed to cause China Company #1 to pay XIAORONG YOU for her involvement in the conspiracy and to help her obtain the Thousand Talent annual award and the Yishi-Yiyi award from the Chinese government using the stolen TSI as the basis for XIAORONG YOU's application to each award program.

17. Co-Conspirator #1 agreed to serve as an intermediary between XIAORONG YOU, on the one hand, and LIU XIANGCHEN and China Company #1, on the other hand, by negotiating with LIU XIANGCHEN and China Company #1 on XIAORONG YOU's behalf, by passing communications between them, by facilitating the transfer of payments from LIU XIANGCHEN and China Company #1 to XIAORONG YOU, and by providing other assistance.

18. XIAORONG YOU, LIU XIANGCHEN, and Co-Conspirator #1 agreed that they

would form a new Chinese company (“China Company #2”) to hold ownership of the stolen TSI, and that each of China Company #1, XIAORONG YOU, LIU XIANGCHEN, and Co-Conspirator #1 would own part of China Company #2.

19. XIAORONG YOU, LIU XIANGCHEN, and Co-Conspirator #1 agreed that they would attempt to enlist the assistance of an Italian company (“Italian Company #1”) in a joint venture with China Company #2, for the purpose of establishing a market presence for China Company #2 in China using Italian Company #1’s established BPA-free manufacturing abilities.

20. XIAORONG YOU, LIU XIANGCHEN, and Co-Conspirator #1 further agreed that after the joint venture with Italian Company #1 had helped established China Company #2 as a China-based manufacturer of BPA-free coatings, China Company #2 would build a laboratory capable of producing second-generation BPA-free coatings with the stolen TSI.

21. XIAORONG YOU, LIU XIANGCHEN, and Co-Conspirator #1 agreed that China Company #2 would then compete with U.S. and foreign companies, including some of the owners of the stolen TSI, in China and elsewhere by selling products designed, developed, and manufactured using the stolen TSI.

OVERT ACTS

In furtherance of the conspiracy and to effect its unlawful objects, the following overt acts, among others, were committed by XIAORONG YOU, LIU XIANGCHEN, and Co-Conspirator #1 in the Eastern District of Tennessee and elsewhere:

22. In or about March 2017, XIAORONG YOU, LIU XIANGCHEN, and Co-Conspirator #1 agreed that XIAORONG YOU would steal TSI in part for the purpose of establishing a Chinese company to manufacture and profit from products developed using the stolen TSI.

23. In or about the summer of 2017, LIU XIANGCHEN and China Company #1 agreed to sponsor XIAORONG YOU's application to China's Thousand Talent Program so that LIU XIANGCHEN and China Company #1 could be paid by the Chinese government for their plan to develop technology that they knew to be based upon stolen TSI.

24. In or about the fall of 2017, LIU XIANGCHEN caused China Company #1 to agree to sponsor XIAORONG YOU's application to China's Yishi-Yiyi project so that LIU XIANGCHEN and China Company #1 could be paid by the Chinese government to develop technology that XIAORONG YOU, LIU XIANGCHEN, and Co-Conspirator #1 knew to be derived from stolen TSI.

25. On or about August 10, 2017, XIAORONG YOU, in exchange for a payment from Employer #1 of approximately \$33,912, signed a written agreement in which she falsely represented to Employer #1 that she had not retained, and no longer had access to, any TSI or confidential information.

26. On or about August 17, 2017, XIAORONG YOU traveled to China for the purpose of defending, with LIU XIANGCHEN's assistance, her application to the Yishi-Yiyi award program using the stolen TSI.

27. On or about August 25, 2017, XIAORONG YOU opened files containing TSI on a computer and took photographs of those TSI files while they were open on the computer screen, to bypass Employer #1's security measures.

28. On or about August 29, 2017 and October 2, 2017, XIAORONG YOU transferred TSI stolen from TSI Owner #1, TSI Owner #2, TSI Owner #3, TSI Owner #4, TSI Owner #5, and TSI Owner #6 to an external hard drive in her possession.

29. On or about September 1, 2017, XIAORONG YOU obtained employment at

Employer #2 in part for the purpose of stealing TSI in furtherance of the conspiracy.

30. From on or about September 17, 2017 through on or about September 21, 2017, XIAORONG YOU traveled from the Eastern District of Tennessee to China for the purpose of defending, with LIU XIANGCHEN's assistance, her application to the Thousand Talents award program using the stolen TSI.

31. On or about October 23, 2017, Co-Conspirator #1 forwarded to XIAORONG YOU a message from LIU XIANGCHEN in which LIU XIANGCHEN stated that he submitted false information to one of the talent programs in order to increase the possible monetary award they could receive.

32. On or about September 29, 2017, October 23, 2017, March 1, 2018, March 7, 2018, April 5, 2018, April 11, 2018, May 24, 2018, May 27, 2018, and May 31, 2018, among other dates, Co-Conspirator #1 forwarded or conveyed to XIAORONG YOU messages from LIU XIANGCHEN made in furtherance of the conspiracy. These facilitated communications pertained to a variety of topics germane to the conspiracy, including the formation of China Company #2, the various equity shares of China Company #2 to be owned by each conspirator, the result of the Thousand Talents award application, the amounts paid by the Yishi-Yiyi award program, building a project team for purposes of expanding the operations of China Company #1, concealing XIAORONG YOU's involvement in the conspiracy to protect her while she remained in the United States, the process of approaching Italian Company #1 to be part of a joint venture, and paying XIAORONG YOU for the work she had already done in furtherance of the conspiracy, among other topics.

33. On or about May 2018, XIAORONG YOU traveled from the Eastern District of Tennessee to China and met with LIU XIANGCHEN for the purpose of presenting market

research to the management of China Company #1, finalizing the terms of a written agreement made in furtherance of the conspiracy and discussing the next steps of the conspiracy, including forming China Company #2 and establishing a joint venture with Italian Company #1.

34. On or about May 7, 2018, XIAORONG YOU and China Company #1, with LIU XIANGCHEN's collaboration, entered into a written "collaboration agreement" setting forth some of the terms of their conspiracy.

35. On or about June 11, 2018, XIAORONG YOU took photos of Employer #2 laboratory equipment located in secure and restricted Employer #2 laboratories in the Eastern District of Tennessee for the purpose of showing LIU XIANGCHEN and others involved in the conspiracy the types of industrial laboratory equipment needed to further the conspiracy.

36. On or about June 21, 2018, XIAORONG YOU, while in the Eastern District of Tennessee, knowing that she was about to be fired from Employer #2, uploaded to her Google drive account, by wire transmission in interstate or foreign commerce, files containing TSI that she had stolen from Employer #2.

37. On or about June 21 and June 22, 2018, XIAORONG YOU, for the purpose of deceiving Employer #2, represented falsely to Employer #2 that XIAORONG YOU had not retained copies of confidential information containing TSI owned by Employer #2.

38. On or about June 22, 2018, XIAORONG YOU, while working for Employer #2 and living in the Eastern District of Tennessee, knowingly possessed an external hard drive containing TSI stolen from TSI Owner #1, TSI Owner #2, TSI Owner #3, TSI Owner #4, TSI Owner #5, TSI Owner #6, and Employer #2 with the intent to use that TSI to the detriment of its owners.

39. On or about the evening of June 22, 2018, XIAORONG YOU, having been caught in possession of stolen TSI, attempted unsuccessfully to cause a representative of Employer #2 to destroy evidence that XIAORONG YOU had copied stolen TSI to the external hard drive in her possession.

All in violation of 18 U.S.C. § 1832(a)(5).

COUNTS TWO – EIGHT
(Theft of Trade Secrets, 18 U.S.C. § 1832(a)(3))

40. Paragraphs 1 through 39 are incorporated herein by reference and re-alleged as though fully set forth in the following counts.

41. On or about June 22, 2018, in the Eastern District of Tennessee, XIAORONG YOU, with intent to convert the trade secrets identified in the chart below, each of which was related to a product and service used in and intended for use in interstate and foreign commerce, to the economic benefit of persons other than the trade secret owner specified in the chart below, and intending and knowing that the offense would injure the owner specified in the chart below, knowingly possessed such information, knowing the same to have been stolen and appropriated, obtained, and converted without authorization:

Count	Owner	Trade Secret	Approximate Cost to Develop
(2)	TSI Owner #1	A formulation for a BPA-free coating for use inside cans (<i>i.e.</i> , beer or other beverage cans) that prevents the contents of the can from interacting with the metal surface of the can over time, owned by TSI Owner #1.	\$7,300,000
(3)	TSI Owner #2	The chemical substances used to create a substitute for epoxy coatings containing BPA, owned by TSI Owner #2.	\$1,500,000

(4)	TSI Owner #3	Newly-developed BPA-free polyolefin dispersion coatings for the inside of food and drink cans, such as aluminum soda cans, that protect both the can from corrosion and its contents from contamination by the can's material, owned by TSI Owner #3	\$25,000,000
(5)	TSI Owner #4	Formulas used to develop BPA-free interior sprays for aluminum and steel food and beverage cans, owned by TSI Owner #4.	\$39,000,000
(6)	TSI Owner #5	The development of BPA-free liquid coating compositions for forming FDA-compliant and EU-compliant, food-contact-safe coatings on the surfaces of metal beverage cans and in the development of analogous coatings for metal food cans, owned by TSI Owner #5.	\$30,000,000
(7)	TSI Owner #6	Information used in the process of developing "Gen-2," BPA-free coating technologies for aluminum food-grade beverage containers, owned by TSI Owner #6.	\$3,800,000
(8)	Employer #2	Resins for use in BPA-free coatings for the interior of rigid metal packaging, owned by Employer #2.	\$13,000,000

Each count being in violation of 18 U.S.C. § 1832(a)(3).

COUNT NINE
(Wire Fraud, 18 U.S.C. § 1343)

42. Paragraphs 1 through 39 are incorporated herein by reference and re-alleged as though fully set forth in the following counts.

43. From on or about June 21, 2018 to on or about June 22, 2018, in the Eastern District of Tennessee, the defendant, XIAORONG YOU, having devised and intending to devise a scheme to defraud, and to obtain money and property by means of materially false or fraudulent pretenses, representations, and promises, transmitted and caused to be transmitted by means of wire communication in interstate and foreign commerce writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice; that is, XIAORONG

YOU uploaded trade secret information owned by Employer #2 by means of wire communication in interstate commerce to XIAORONG YOU's personal Google Drive account, and then represented falsely to Employer #2 that XIAORONG YOU had not retained copies of trade secret information owned by Employer #2, in violation of 18 U.S.C. § 1343.

* * * * *

A True Bill:




Foreperson

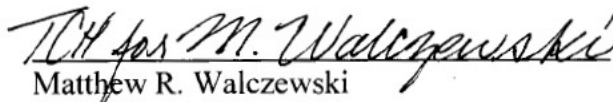
Approved:

J. Douglas Overbey
United States Attorney

By:


Timothy C. Harker
Assistant United States Attorney

By:


Matthew R. Walczewski
Trial Attorney, National Security Division
U.S. Department of Justice

CRIMINAL CASE COVER SHEET

U.S. ATTORNEY'S OFFICE

Defendant Name: XIAORONG YOU aka SHANNON YOU
LIU XIANGCHEN

19-14
JRG 2

Place of Offense (City & County): Kingsport / Sullivan County

Juvenile: Yes No Matter to be Sealed: Yes No

Interpreter: No Yes Language: Mandarin

Total # of Counts: Petty Misdemeanor (Class) 9 Felony

ORIGINAL INDICTMENT		Count(s)
U.S.C. Citation(s) and Description of Offense Charged		
	Conspiracy to Commit Theft of Trade Secrets (18 U.S.C. § 1832(a)(5))	1
	Theft of Trade Secrets (18 U.S.C. § 1832(a)(3))	2 - 8
	Wire Fraud (18 U.S.C. § 1343)	9

Current Trial Date (if set): _____ before Judge _____

Criminal Complaint Filed: No Yes

Defendant on Supervised Release: Yes No

Violation Warrant Issued? No Yes Case No. _____

Related Case(s):

Case Number	Defendant's attorney	How related
-------------	----------------------	-------------

Criminal Informations:

Pending criminal case: No Yes Case No. _____

New Separate Case _____ Supersedes Pending Case _____

Name of defendant's attorney: _____

Retained: _____ Appointed: _____

Date: September 12, 2017 Signature of AUSA: s/ Timothy C. Harker

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT GREENEVILLE

UNITED STATES OF AMERICA)
)
)
v.) No. 2:19-CR-14
)
XIAORONG YOU)

MEMORANDUM OPINION AND ORDER

This matter is before the Court prior to Defendant’s sentencing. The parties dispute the amount of loss Defendant intended as the result of her criminal conduct, and this dispute must be resolved before the Court can sentence Defendant in this case. For the following reasons, the Court determines the applicable amount of loss in this case to be \$121,800,000 USD.

I. BACKGROUND

In paragraph 24 of Defendant’s PSR, the Probation Office states that “[a] conservative total cost of developing trade secrets in this case [is] \$121.1 million. If the loss is more than \$65,000,000 but less than \$150,000,000 increase by 24 levels. USSG §2B1.1(b)(1)(M).” Both parties, however, disagree with using research and development costs as an estimate of loss.

The Government seeks a higher value of intended loss, based largely on representations made by the Defendant in grant applications before the Chinese government. The Government cites Defendant’s Thousand Talent Plan Application (“TTP Application”), which was submitted to the Chinese government in June 2017. The Government contends that the TTP Application establishes the following: (1) Defendant understood global can-coatings sales to be approximately \$7.7B, with sales in China specifically accounting for \$2.9B, or 38% of the global market; (2) Defendant believed her new company would obtain a 3% to 5% market share with annual sales of

\$102.5M to \$131.7M from 2021-2023; (3) can coating production would eventually increase to sales of \$292.8M to \$351.4M annually from 2024-2027; (4) Defendant intended to earn not less than \$1.478B in revenue by selling into the global and Chinese markets between 2021 to 2027; and (5) Defendant intended to “break[] through both green and technical international trade barriers” to “earn a share of the global market,” as well as “break the international monopoly [on can coatings].” [Doc. 392, at 6–11]. The Government accordingly calculates that Defendant’s future sales were estimated to be between \$1.48B to \$1.8B. [*Id.* at 9]. Ultimately, however, the Government argues for a “conservative” estimated loss number based on representations made in a PowerPoint that the Defendant would pay approximately \$220M in taxes at an estimated 100% tax rate to the Chinese government between 2021 and 2027. [*Id.* at 17–19].

Defendant, on the other hand, argues that the Government has failed to prove any amount of intended loss by a preponderance of the evidence. [*See* Doc. 400]. She points out that there has been no independent, unbiased testimony regarding the value of the trade secrets in this case. Rather, the Government called upon employees of the victim companies to testify. Additionally, Defendant argues that: (1) she never disclosed or shared the trade secret information; and (2) the grant applications to the Chinese government are not indicative of purposeful intent to harm the seven victim companies because they are puffery and ambitious speculation.

II. LEGAL STANDARD

U.S.S.G. § 2B1.1(b)(1) enhances fraud sentences based on “loss.” Under a Guidelines comment, “intended loss” is defined as “the pecuniary harm that the defendant purposely sought to inflict,” and “includes intended pecuniary harm that would have been impossible or unlikely to

occur[.]” See U.S.S.G. § 2B1.1 cmt. n.3(A)(ii).¹ In creating this definition, the Commission adopted the interpretation of “intended loss” articulated in *United States v. Manatau*, 647 F.3d 1048 (10th Cir. 2011). U.S.S.C., *Amendments to the Sentencing Guidelines* (Apr. 30, 2015), at 24–25. There, the Tenth Circuit held that “[i]ntended loss’ means the loss the defendant *purposely* sought to inflict” and therefore “does not mean a loss that the defendant merely *knew* would result from his scheme or a loss he might have *possibly and potentially* contemplated.” 647 F.3d at 1050 (emphasis in original).

Thus, courts in multiple circuits have found that in trade secrets cases, the “[i]ntended loss analysis, as the name suggests, turns upon how much loss the defendant actually intended to impose’ on the victim, regardless of whether the loss actually materialized or was even possible.” *United States v. Xue*, No. 16-22, 2020 U.S. Dist. LEXIS 173410, at *40–*42 (E.D. Pa. Sept. 22, 2020) (citing *United States v. Pu*, 814 F.3d 818, 824 (7th Cir. 2016)) (citations partially omitted).

“For purposes of U.S.S.G. § 2B1.1, the government bears the burden to prove the amount of loss—actual or intended—by a preponderance of the evidence.” *United States v. Riccardi*, 989 F.3d 476, 481 (6th Cir. 2021). In the Sixth Circuit, district courts need not reach an exact figure for the loss a victim suffered or the amount of harm a defendant caused or intended to cause; a “reasonable estimate” will do. *United States v. Howley*, 707 F.3d 575, 582 (6th Cir. 2013) (citing U.S.S.G. § 2B1.1, cmt. n.3(C)). The Sixth Circuit will only reverse “clearly erroneous estimates.” *Id.* (citing *United States v. Warshak*, 631 F.3d 266, 328 (6th Cir. 2010)).

¹ The Third Circuit has noted that “[o]nly this comment, not the Guidelines’ text, says that defendants can be sentenced based on the losses they intended. By interpreting ‘loss’ to mean intended loss, it is possible that the commentary sweeps more broadly than the plain text of the Guideline.” *United States v. Kirschner*, 995 F.3d 327, 333 (3d Cir. 2021) (citing *United States v. Nasir*, 982 F.3d 144, 177 (3d Cir. 2020) (en banc) (Bibas, J., concurring)).

In estimating a loss, a comment to the Guidelines states that “the estimate of the loss shall be based on available information, taking into account, as appropriate and practicable under the circumstances, factors such as the following: (i) The fair market value of the property unlawfully taken, copied, or destroyed; or, if the fair market value is impracticable to determine or inadequately measures the harm, the cost to the victim of replacing that property; (ii) in the case of proprietary information (e.g., trade secrets), the cost of developing that information or the reduction in the value of that information that resulted from the offense; (iii) the cost of repairs to damaged property; (iv) the approximate number of victims multiplied by the average loss to each victim; (v) the reduction that resulted from the offense in the value of equity securities or other corporate assets; and (vi) more general factors, such as the scope and duration of the offense and revenues generated by similar operations.” U.S.S.G. § 2B1.1 cmt. n.3(C)(i)–(ii).

III. ANALYSIS

a. Sixth Circuit Precedent Requires This Court to Find an Amount of Loss

In *United States v. Howley*, the Sixth Circuit vacated two defendants’ sentences and remanded to the district court for further proceedings to determine an intended loss amount. 707 F.3d at 583. The Court’s main issue with the district court’s decision was that the district court concluded that there was no calculable intended loss in the case:

Without further explanation, the court found that the government had failed to establish any loss at all, notwithstanding beyond-a-reasonable-doubt convictions premised on the reasonable assumption that the Goodyear design—the underlying trade secret—was worth something. Nor was the district court’s no-loss finding insignificant. Even the smallest loss the government argued for, \$305,000, would have yielded a guidelines range of 37 to 46 months in prison. In the absence of any loss, Roberts and Howley faced a guidelines range of 4 to 10 months. The district court imposed sentences of four months of home confinement, 150 hours of community service and four years of probation for each defendant.

The amount of loss was a contested and high-stakes factual question, making it imperative that the district court “engage[] in a more thorough explication

of its calculation.” Without more, the district court’s zero-loss finding seems at odds with the defendants’ convictions for stealing property that had “independent economic value.” If the district court were dissatisfied with the government’s estimates, it could have generated its own. The court, for instance, could have accepted the defendants’ argument that they intended to deprive Goodyear only of part of the value of the swabbing-down machine, not the full value, and arrived at an estimate that represented a percentage of the machine’s total cost. Or it could have asked the parties to present additional evidence. The ultimate decision is up to the district court, which is in a “unique position,” to assess the losses [the defendants] intended to cause. **All we require is that the court provide reasons for its choice.**

On remand, the district court need not be exacting. **The Guidelines require only a “reasonable” estimate of actual or intended loss within broad ranges. But the court must at least provide an estimate and reasons for it.** Nor need a loss estimate above zero necessarily tie a sentencing judge’s hands. Yes, all else being equal, an estimate of a substantial loss necessarily will increase the guidelines range, but it will not override the district court’s duty to exercise discretion in deciding what sentences to impose on the defendants, whether within the guidelines range or outside of it.

Id. at 582–83 (emphasis added).

While the Sixth Circuit has not directed this Court to apply any particular methodology to calculate an amount of intended loss, one thing is clear: the Court must reach a non-zero determination on the amount. Indeed, when the *Howley* case was remanded back to the district court for further consideration, Judge Phillips noted the following during re-sentencing:

Based on the parties’ submissions and the testimony presented today, the Court finds that the most reasonable estimate of the loss in this case is the research and development cost to Goodyear, which the Court will determine the amount very shortly.

...

Consequently, it’s almost impossible for the Court to come up with an accurate determination as to the amount of loss to Goodyear.

The Sixth Circuit has indicated that we do not have to come up with an exact amount. The Sixth Circuit stated that, “On remand, the district court need not be exacting. The guidelines require only a reasonable estimate of actual or intended loss within broad ranges. Therefore, it’s the determination of the Court that the amount of loss occasioned by Goodyear is between 200,000 or \$500,000.”

[Doc. 225 in Case No. 3:08-cr-175, at 70–71 (emphasis added)]. Accordingly, the Court must reject Defendant’s argument that the loss amount in this case should be zero.

b. The Court Will Determine a Loss Amount Based on Anticipated Profits

The Court agrees with the parties that probation’s estimation of intended loss, based on the cost of development of the trade secrets at issue, is inappropriate. The Court is mindful of the fact that it must determine an amount of loss that Defendant “‘*purposefully* sought to inflict,” rather than a loss Defendant “‘merely *knew* would result from h[er] scheme or a loss [s]he might have *possibly and potentially* contemplated.” *Manatau*, 647 F.3d at 1050 (emphasis in original); U.S.S.C., *Amendments to the Sentencing Guidelines* (Apr. 30, 2015), at 24–25. Evidence in the record suggests that additional work would still be needed to develop a competitive product based on the misappropriated trade secrets, and based on the representations made in her grant applications, Defendant clearly intended to enter the monopolistic can-coating market and make a profit. Accordingly, a finding that Defendant intended to cause the victim companies a dollar-for-dollar loss equal to the amount of research and development funds expended in developing the victim companies’ BPA-free coatings is improper here. In reaching a determination of intended loss, the Court will rely on other “available information” established during trial, as is permitted by the Guidelines.²

The Court agrees with the Government that in a monopoly market such as this, anticipated profits are the most reasonable measure of loss. Defendant readily acknowledged in her grant application that the current can-coating industry is, indeed, a monopoly run by the victim

² “[O]f course, in analyzing the defendant’s *mens rea* the district court ‘is free . . . to make reasonable inferences about the defendant’s mental state from the available facts.’” *United States v. Shi*, No. 17-cr-110, 2019 U.S. Dist. LEXIS 218106, at *5 (D.D.C. Dec. 17, 2019) (citing *Manatau*, 647 F.3d at 1056).

companies that she “anticipated to break.” [Doc. 392, at 12]. Therefore, it follows that whatever existing market share Defendant intended to gain, she intended to take it from a victim company. After all, Defendant can only gain existing market share if the victim companies forming the monopoly lose that amount of the market. However, the Court also agrees with Defendant that the profit and tax estimates put forth in materials such as presentations or grant applications are likely inflated as a result of puffery and based on speculation. The Court is bound to determine the amount of loss Defendant intended to inflict, not an amount of loss she “might have *possibly and potentially* contemplated.” *Manatau*, 647 F.3d at 1050 (emphasis in original). Therefore, the Court rejects the Government’s proffered value of intended loss, based on projected tax payments to the Chinese government, as well. To calculate the Defendant’s intended amount of loss, the Court must look elsewhere.

It is important to remember that the trade secrets at issue involved BPA-free coatings, which have not been adopted universally, and there is no indication in the record that they will be adopted universally in the future. [Doc. 309, at 38–40; Doc. 314, at 94–95]. Dan Leschnik, Global Technical Manager for Akzo-Nobel, testified that AkzoNobel has approximately 50% of the global market share for internal can coatings, and approximately 60% to 65% of that same market specifically in China. [Doc. 309, at 14, 46]. However, Mr. Leschnik also testified that AkzoNobel’s sales in China were “99 percent BPA and 1 percent BPA-free” at the time of trial. [Doc. 310, at 15]. So, despite having 60 to 65% of the Chinese market, only 1% of AkzoNobel’s sales there involved BPA-free coating technologies—the trade secrets at issue in this case. David Bem, Chief Technology Officer at PPG Industries, further testified that PPG readily sold BPA coatings in China but had only begun to make BPA-free sales in the last twelve months as of the time of trial. [Doc. 314, at 95].

Further, testimony at trial showed that while there are approximately 60 billion cans in the Chinese market, approximately 60% of those cans are consumed by local, state-owned beer companies. [Doc. 309, at 74]. Typically, global brands prefer to buy from global can makers, and global can makers prefer to buy their coatings from global suppliers, like the victim companies in this case. [*Id.* at 73–74]. However, Chinese state-owned can makers would likely prefer to buy coatings from Chinese suppliers, were they available. [*Id.* at 63–64, 76; Doc. 341, at 16; Doc. 342, at 17].

Calculations with respect to the portion of the global market share Defendant intended to take are too speculative. The only information the Court has to this effect is that Defendant reported the total value of the can-coating market to be over \$7 billion dollars annually in her TTP Application, and her projections anticipated that her new company would take 3% to 5% of the market share. As explained before, the Court finds this projection unreliable, as it is likely the result of puffery and speculation intended to entice the Chinese government into issuing a grant to Defendant and her co-applicants. Further, the Court is not aware of information available in the record regarding global sales of BPA-free versus BPA can coatings, or more importantly, how much of Defendant’s intended total gains in market share would come from the global market versus the Chinese market specifically.

However, the Court does have information available in order to estimate Defendant’s intended gains in the Chinese market. Based on the testimony of Dan Leschnik, the Court finds it is reasonable to assume that a conservative percentage of the existing market share in China for BPA-free coating sales would be 1% of the total market. Defendant’s stated intent was to “fill the gap in Asia,” which includes the Chinese market for can coatings. As previously discussed, due to the monopolistic nature of the market, Defendant could only gain existing market share in China

by taking it from one of the victim companies. Therefore, it follows that Defendant's intended gains in the Chinese market must be equivalent to the loss she intended to one or more of the victim companies.

The Court cannot attempt to guess how much of the can-coating market, in China or otherwise, will eventually shift to BPA-free coatings, or whether the can-coating market will grow further as a whole. However, the Court can determine a baseline for Defendant's intended gains in the Chinese market based on the state of the market that existed at the time she was looking to set up her own operation in China. The total Chinese market for can coatings is estimated at \$2.9 billion USD annually. If 60% of can makers in the Chinese market are Chinese, then local-owned Chinese purchasing power for can coatings represents \$1.74 billion USD of the Chinese market. As previously established, these businesses would likely prefer to buy from a domestic coating manufacturer, of which Defendant would have been the first of her kind.

Of that \$1.74 billion USD in purchasing power, however, only 1% of sales in the Chinese market as it existed around the time Defendant sought to enter it were for BPA-free coatings. This means that the total available amount of existing market for BPA-free coating sales is only \$17.4 million USD annually. Therefore, if Defendant were to "fill the gap in Asia" and absorb all purchases of BPA-free coatings from Chinese-owned can makers, she would stand to bring in sales of \$17.4 million USD a year on the back of the trade secrets she misappropriated. Over an estimated seven years of profit, from 2021 to 2027, this would lead to a sales total of \$121.8 million USD.

There are, of course, assumptions being made in this calculation. One is that the demand for BPA-free coatings in the Chinese market will neither grow nor shrink. Another is that, as a local can-coating manufacturer, Defendant would in fact absorb all sales from Chinese-owned can

makers. There is also no way to guarantee that any Chinese can manufacturer currently accounts for purchases of BPA-free coating in China, or that to the extent it exists, such demand will continue in the future. However, district courts need not reach an exact figure for the amount of harm a defendant caused or intended to cause; in fact, the Court finds that such an exact calculation would be impossible in this case. Thankfully for this Court, a “reasonable estimate” of intended losses will do. *Howley*, 707 F.3d at 582 (6th Cir. 2013). The Court finds that based on available information, including Defendant’s intent to gain existing market share in a monopoly, and as established by a preponderance of the evidence, \$121.8 million USD is a conservative and reasonable estimate of Defendant’s intended losses to the victim companies in order to “break” the can-coating monopoly and “fill the gap in Asia.”

IV. CONCLUSION

The Court finds that Defendant’s intended losses in this case are \$121,800,000 USD. If the loss is more than \$65,000,000 but less than \$150,000,000 increase by 24 levels. USSG §2B1.1(b)(1)(M).

So ordered.

ENTER:

s/J. RONNIE GREER
UNITED STATES DISTRICT JUDGE



REPORTING INTELLECTUAL PROPERTY CRIME

A Guide for Victims of Copyright Infringement, Trademark Counterfeiting, and Trade Secret Theft

Third Edition





REPORTING INTELLECTUAL PROPERTY CRIME

A Guide for Victims of Copyright Infringement, Trademark Counterfeiting, and Trade Secret Theft

Third Edition

Table of Contents

What Are Copyrights, Trademarks, and Trade Secrets?	3
How Can Intellectual Property Be Stolen?	3
When Is an Intellectual Property Violation a Federal Crime?.....	4
Why Should You Report Intellectual Property Crime?	6
What Should You Do If You Are Victimized?.....	8
Where Do I Report an Intellectual Property Crime?.....	10
Federal Investigative Contacts	10
State and Local Investigative Contacts	12
Prosecution Contacts.....	13
How Can You Assist Law Enforcement?.....	14
Checklist for Reporting an Intellectual Property Crime	15
Criminal Copyright and Trademark Infringement	16
Trade Secret Offenses.....	20
Additional Resources	26

Note: The information contained in this document is a general guide for victims of intellectual property crime. This document is not intended to create or confer any rights, privileges, or benefits to prospective or actual witnesses or defendants. In addition, this document is not intended as a United States Department of Justice directive or as a document that has the force of law.

What Are Copyrights, Trademarks, and Trade Secrets?

The United States has created enforceable rights in “intangibles” that are known as intellectual property, including copyrights, trademarks, and trade secrets. **Copyright law** provides federal protection against infringement of certain exclusive rights, such as reproduction and distribution, of “original works of authorship,” including computer software, literary works, musical works, and motion pictures. 17 U.S.C. §§ 102(a), 106. The use of a commercial brand to identify a product is protected by **trademark law**, which prohibits the unauthorized use of “any word, name, symbol, or device” used by a person “to identify and distinguish his or her goods, including a unique product, from those manufactured or sold by others and to indicate the source of the goods.” 15 U.S.C. § 1127. Finally, **trade secret law** prohibits the unauthorized disclosure of any confidential and proprietary information, such as a formula, device, or compilation of information but only when that information possesses an independent economic value because it is secret and the owner has taken reasonable measures to keep it secret. 18 U.S.C. §§ 1831, 1832. For more information on these rights and how they are criminally enforced, see Prosecuting Intellectual Property Crimes (4th ed. 2013), U.S. Department of Justice, Computer Crime and Intellectual Property Section (www.justice.gov/criminal-ccips/ccips-documents-and-reports).

How Can Intellectual Property Be Stolen?

Intellectual property can be stolen (*i.e.*, infringed or misappropriated) in many ways. For example, copyrighted works, such as movies, music, books, software or games, may be illegally infringed by reproducing or distributing unauthorized copies of such works either online or by manufacturing and distributing infringing CDs or DVDs containing the unauthorized content. A trademark or service mark may be infringed by offering goods, services, labels or other packaging containing a counterfeit mark. A trade secret can be surreptitiously misappropriated from its owner either by a company insider or by someone outside a company and used to benefit the thief, a competitor, or other third party.

When Is an IP Violation a Federal Crime?

Although individuals or companies can pursue civil remedies to address violations of their intellectual property rights, criminal sanctions are often warranted to ensure sufficient punishment and deterrence of wrongful activity. Congress has continually expanded and strengthened criminal laws for violations of intellectual property rights to protect innovation, to keep pace with evolving technology and, significantly, to ensure that egregious or persistent intellectual property violations do not merely become a standard cost of doing business for defendants. In most instances, the statutes of limitations for intellectual property crime is five years, but may be extended in some circumstances, such as an ongoing or continuing crime. Among the most significant criminal provisions are the following:

- ❑ **Counterfeit Trademarks:** The Trademark Counterfeiting Act, 18 U.S.C. § 2320(b)(1)(A), provides penalties of up to ten years' imprisonment and a \$2 million fine for a defendant who intentionally "traffics in goods or services and knowingly uses a counterfeit mark on or in connection with such goods or services," or intentionally "traffics in labels, . . . documentation, or packaging . . . knowing that a counterfeit mark has been applied thereto." Section 2320(b)(3) provides penalties of up to twenty years' imprisonment and a \$5 million fine for a defendant who intentionally traffics in counterfeit drugs or certain counterfeit military goods or services.
- ❑ **Counterfeit Labeling:** The counterfeit labeling provisions of 18 U.S.C. § 2318 prohibit trafficking in counterfeit labels designed to be affixed to movies, music, software, and literary, pictorial, graphic, or sculptural works and works of visual art as well as trafficking in counterfeit documentation or packaging for such works. Violations are punishable by up to five years' imprisonment and a \$250,000 fine.
- ❑ **Criminal Copyright Infringement:** Copyright infringement is a felony punishable by up to three years' imprisonment and a \$250,000 fine under 17 U.S.C. § 506(a) and 18 U.S.C. § 2319 where a defendant willfully *reproduces* or *distributes* at least ten copies of one or more copyrighted works with a total retail value of more than \$2,500 within a 180-day period. The maximum penalty rises to five years' imprisonment if the defendant also acted "for purposes of commercial advantage or private financial gain." Misdemeanor copyright infringement occurs where the value exceeds \$1,000 or where the defendant willfully violated any of the exclusive rights "for purposes of commercial advantage or private financial gain."

- ❑ **Pre-Release Criminal Copyright Infringement:** Pre-release piracy, *i.e.*, willful infringement “by the distribution of a work being prepared for commercial distribution, by making it available on a computer network accessible to members of the public, if such person knew or should have known that the work was intended for commercial distribution,” is a felony punishable by up to three years’ imprisonment and a \$250,000 fine under 17 U.S.C. § 506(a)(1)(C) and 18 U.S.C. § 2319(d). The maximum penalty rises to five years’ imprisonment if the defendant also acted “for purposes of commercial advantage or private financial gain.”

- ❑ **Theft of Trade Secrets:** The Economic Espionage Act contains two separate provisions that criminalize the theft of trade secrets. The first provision, 18 U.S.C. § 1831, prohibits the theft of trade secrets for the benefit of a foreign government, instrumentality, or agent, and is punishable by up to 15 years’ imprisonment and a \$5,000,000 fine. The second, 18 U.S.C. § 1832, prohibits the commercial theft of trade secrets to benefit someone other than the owner, and is punishable by up to ten years’ imprisonment and a \$250,000 fine. The penalties are higher for defendants who are companies. The statute broadly defines the term “trade secret” to include all types of information that the owner has taken reasonable measures to keep secret and that itself has independent economic value. 18 U.S.C. § 1839(3). Federal law also provides special protections to victims in trade secret cases to ensure that the confidentiality of trade secret information is preserved during the course of criminal proceedings. Specifically, the statute expressly states that courts “shall enter such orders and take such action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws.” 18 U.S.C. § 1835(a); *see also* Levine & Flowers, [How Prosecutors Protect Trade Secrets](#), 38 Am. J. Trial Advoc. 461 (2014-2015).

- ❑ **Camcording:** The Family Entertainment and Copyright Act criminalizes the use of camcorders and similar devices to record movies playing in public theaters. “Camcording” is a felony punishable by up to three years imprisonment’ and a \$250,000 fine under 18 U.S.C. §2319B(a) where a defendant “knowingly uses or attempts to use an audiovisual recording device to transmit or make a copy of a motion picture. . . in a motion picture exhibition facility.”

- ❑ **Additional Charges:** Where appropriate, prosecutors may respond to intellectual property crime with additional charges, such as Wire Fraud (18 U.S.C. § 1343), Mail Fraud (18 U.S.C. § 1341), Computer Fraud and Abuse Act (18 U.S.C. § 1030), and Smuggling (18 U.S.C. § 545).

Why Should You Report Intellectual Property Crime?

Intellectual property is an increasingly important part of the United States economy, representing its fastest growing sector, contributing billions of dollars to America's gross domestic product, and employing over 45 million Americans, according to the Global Intellectual Property Center. See www.theglobalipcenter.com. As the nation continues to shift from an industrial economy to an information-based economy, the assets of the country are increasingly based in intellectual property. In addition, intellectual property crime in the United States and abroad not only threatens our nation's economic well-being, it can also place at risk the public health and safety of our citizens and our national security.

In recognition of this trend, the Department of Justice is waging an aggressive campaign against intellectual property crime in all its forms. For more information on the Department's efforts, see the Department's Annual PRO IP Act Reports. See www.justice.gov/criminal/cybercrime/documents.html.

Effective prosecution of intellectual property crime, however, also requires substantial assistance from its victims. Because the victims of intellectual property crime are often in the best position to detect a theft, law enforcement authorities cannot act in many cases unless the crimes are reported in the first place. Once these crimes are reported, federal law enforcement authorities need to quickly identify the facts that establish jurisdiction for the potential intellectual property offenses, such as federal copyright and trademark registration information, as well as facts concerning the extent of a victim's potential loss, the nature of the theft, and possible suspects. In a digital world where evidence can disappear at the click of a mouse or the tap of a smartphone, federal law enforcement has the ability to quickly preserve digital evidence in more than 80 countries. Federal law enforcement also has the ability to deter foreign IP criminals by extraditing them to the U.S. for prosecution, assisting in a foreign prosecution, or by supporting the imposition of diplomatic responses, such as sanctions or blacklisting.

Accordingly, the Department of Justice has created this guide for victims to facilitate the flow of critical information from victims of intellectual property crimes to law enforcement authorities. The Department of Justice's goal is to make it as easy as possible to report incidents of intellectual property crime to law enforcement authorities, including whom to contact and what to tell them.

Note: The guidelines set forth below seek information that, in the experience of Department of Justice prosecutors and investigators, is useful or even critical to the successful prosecution of the most common intellectual property crimes. These guidelines are not intended to be exhaustive, nor does the presence or absence of responsive information from the victim necessarily determine the outcome of an investigation.

What Should You Do If You Are Victimized?

Victims of intellectual property crime, such as copyright infringement, trademark counterfeiting, and theft of trade secrets, often conduct internal investigations before referring matters to law enforcement. These investigations can encompass a variety of steps, including interviewing witnesses, acquiring samples of the counterfeit goods, conducting surveillance of suspects, and examining computers and other evidence. Victims can maximize the benefit of these independent investigative activities as follows:

- ❑ **Document All Investigative Steps:** To avoid duplication of effort and retracing of steps, internal investigations should seek to create a record of all investigative steps that can later be presented to law enforcement, if necessary, including the names, titles and contact information of persons with knowledge of each step. If a victim company observes counterfeit goods for sale online and makes a purchase, for example, investigators should record the domain name, URL, and IP address of the website, the date and time of the purchase, the method of payment, and the date and manner of delivery of the goods. Any subsequent examination or testing of the goods should then be recorded in a document that identifies the telltale characteristics of theft or specific indicators of counterfeiting, such as lack of a security seal, poor quality, failure to meet specifications, packaging, or the like.

Similarly, in the case of a suspected theft of trade secrets, any internal investigation or surveillance of the suspect, or a competitor believed to be using the stolen information, should be recorded. Records of any interviews with suspects or witnesses should be made by tape or in writing. The pertinent confidentiality agreements, security policies, and access logs should also be gathered and maintained to facilitate review and reduce the risk of deletion or destruction.

- ❑ **Preserve the Evidence:** Any physical, documentary, or digital evidence acquired in the course of an internal investigation should be preserved for later use in a legal proceeding. In the online theft example identified above, victims should print out or obtain a digital copy of the offending website, preserve any e-mails or texts related to the counterfeit item(s), and safely store any infringing goods and their packaging, which may contain details of their origin. Additionally, print out and preserve any documentation of the course of dealing with the offending seller, including (but not limited to) any sales agreements or contracts, communications about the purchase, or other such documentation. If the computer of an employee suspected of stealing trade secrets has been seized,

any forensic analysis should be performed on a copy of the data, or “digital image,” to refute claims that the evidence has been altered or corrupted.

- ❑ **Contact Law Enforcement Right Away:** Victims can maximize their legal remedies for intellectual property crime by making contact with law enforcement soon after its detection. Early referral to law enforcement is the best way to ensure that evidence of an intellectual property crime is properly secured and that all investigative avenues are fully explored, such as the execution of search warrants and possible undercover law enforcement activities. Communication with law enforcement authorities at the onset of suspected violations also allows a victim to coordinate administrative or civil proceedings with possible criminal enforcement. Use the reporting checklists set forth later in this guide to organize the information you gather and provide the necessary information to your law enforcement contact.

Where Do I Report an Intellectual Property Crime?

Although there are a variety of ways to report an intellectual property crime to law enforcement, the following list identifies the most common and efficient investigative and prosecutorial contacts.

Federal Investigative Contacts

- ❑ **National Intellectual Property Rights Coordination Center (“IPR Center”).** The IPR Center is an interagency task force led by U.S. Immigration and Customs Enforcement, Homeland Security Investigations (“ICE-HSI”). The IPR Center is a collaborative effort by over 19 U.S. government investigative and regulatory agency partners, including the Federal Bureau of Investigation (“FBI”), as well as representatives from Interpol, Europol, Canada and Mexico, that work together to combat intellectual property crime. IPR Center partners work together to investigate and deconflict case leads, interdict counterfeit and pirated goods at the borders, and provide extensive training and outreach. The IPR Center also works closely with the Department of Justice through the Criminal Division’s Computer Crime and Intellectual Property Section. The IPR Center encourages victims to visit its website at www.IPRCenter.gov to obtain more information about the IPR Center and to report violations of intellectual property rights online or by emailing IPRCenter@dhs.gov. You can also report IP crime by clicking on The IPR Center’s “Report IP Theft” button.
- ❑ **Federal Bureau of Investigation (“FBI”).** The FBI’s Criminal Investigative Division’s Intellectual Property Rights Unit (“IPRU”) oversees its national intellectual property rights program, which includes dedicated FBI Special Agents responsible for investigating (i) thefts of trade secrets, (ii) manufacturing and trafficking in counterfeit goods, and (iii) IPR infringement, which causes significant economic impact. The IPRU is headquartered at the IPR Center, and the FBI Special Agents dedicated to investigating IP crime are located in field offices throughout the country. The IPRU’s agents work closely with all FBI field offices to combat IP crime. The FBI’s IPRU encourages victims to report intellectual property crimes through the IPR Center or to any of the FBI’s 56 field offices and 63 international legal attaches. Rights holders are also encouraged to develop a relationship with an FBI agent in a local field office *before* an incident



occurs. A list of the FBI field offices is available online at www.fbi.gov/contact-us/field/field-offices.

- ❑ **Internet Crime Complaint Center (“IC3”).** IC3 is a partnership between the FBI, the National White Collar Crime Center, and the Department of Justice’s Bureau of Justice Assistance. IC3 receives, develops, and refers criminal complaints involving a range of cybercrimes including intellectual property crime occurring online. IC3 encourages victims to report complaints involving cybercrime through its website at www.ic3.gov.

- ❑ **U.S. Food and Drug Administration—Office of Criminal Investigations (“OCI”).** OCI protects the public health and furthers the FDA mission by investigating suspected criminal violations of the Federal Food, Drug, and Cosmetic Act (“FDCA”) and other related laws. Among other things, OCI investigates breaches in the legitimate medical supply chain by individuals and organizations dealing in unapproved, counterfeit, and substandard medical products. Those who work in the pharmaceutical industry should be aware that the Drug Supply Chain Security Act (“DSCSA”) requires certain trading partners (manufacturers, repackagers, wholesale distributors, and dispensers), to notify FDA and all appropriate immediate trading partners not later than 24 hours after making the determination that a product is illegitimate. Manufacturers are additionally required to notify FDA and appropriate immediate trading partners not later than 24 hours after the manufacturer determines or is notified by FDA or a trading partner that there is a high risk that a product is illegitimate. The DSCSA also requires that manufacturers, repackagers, wholesale distributors, and dispensers consult with FDA before terminating the notification about an illegitimate product.

State and Local Investigative Contacts

Federal, state, and local law enforcement agencies and prosecutors all over the country have formed task forces or other working groups to combat computer and intellectual property crime and to promote information sharing between all levels of law enforcement and industry. A state or local task force may be an appropriate contact for cases that do not meet federal criminal thresholds. Examples of these task forces include:

- ❑ **DOJ-Funded Intellectual Property Enforcement Task Forces.** Since the inception of the program in FY2009, OJP has awarded more than \$26 million in grants to support state and local law enforcement agencies, training and technical assistance providers, and an IP public education campaign. Of this total amount of funding, state and local law enforcement agencies have received more than \$19 million. More information on the grant program is available online at www.bja.gov/ProgramDetails.aspx?Program_ID=64. To determine whether a task force has been funded in a particular area, see the following link to past grant recipients: www.bja.gov/funding.aspx#3.
- ❑ **InfraGard.** The FBI has founded more than 80 chapters of InfraGard – a government and private sector alliance developed to promote the protection of critical information systems – around the country. See www.infragard.net for more information about InfraGard generally and to find your local chapter.
- ❑ **Electronic Crimes Task Forces.** The United States Secret Service (“USSS”) has created Electronic Crimes Task Forces in 40 cities. More information on the USSS and the Electronic Crimes Task Force program can be found at www.secretservice.gov/investigation/.

Prosecution Contacts

Because of the often complex nature of intellectual property crime and the rapid response required by law enforcement, early engagement of prosecutors often can be helpful. Victims can contact Department of Justice prosecutors in the following ways:

- ❑ **Computer Hacking and Intellectual Property (“CHIP”) Coordinators.** Each of the 93 U.S. Attorneys’ Offices throughout the country has at least one Assistant U.S. Attorney who serves as a CHIP coordinator. There are also many districts that have two or more CHIP prosecutors. In total, the Department of Justice has a network of over 270 federal prosecutors who specialize in prosecuting high tech crimes, including intellectual property crimes. The core responsibilities of CHIP prosecutors include (1) prosecuting computer crime and intellectual property offenses; (2) serving as the district’s legal counsel on matters relating to those offenses and the collection of electronic or digital evidence; (3) training prosecutors and law enforcement personnel in the region; and (4) conducting public and industry outreach and awareness activities. Victims can contact CHIP prosecutors in their district by calling the local U.S. Attorney’s Office and asking for the CHIP prosecutor. A list of U.S. Attorneys’ Offices is available online at www.justice.gov/usao/us-attorneys-listing.
- ❑ **Computer Crime and Intellectual Property Section (“CCIPS”).** CCIPS is a section within the Department of Justice’s Criminal Division. CCIPS has a core team of expert IP prosecutors who prosecute IP crimes and help coordinate multi-district and international IP cases. In addition to prosecution, CCIPS attorneys assist in developing and implementing the Department’s overall criminal enforcement strategy to combat intellectual property crime, provide domestic and international training on investigating and prosecuting intellectual property cases, and conduct industry outreach. CCIPS also houses the National CHIP Coordinator to help manage the CHIP Network. In these efforts, CCIPS works closely with the IPTF, U.S. Attorneys’ Offices, CHIP coordinators, the IPR Center, and the FBI, among other agencies. More information about CCIPS is available online at www.cybercrime.gov and at (202) 514-1026.
- ❑ **Intellectual Property Law Enforcement Coordinators (“IPLECs”).** The Department of Justice’s IPLEC program places experienced prosecutors in high-impact regions to enhance individual countries’ capacities to investigate and prosecute IP crimes and to develop regional networks to more effectively deter and detect IP crimes. The Department of Justice currently has regional IPLECs in Romania, Hong Kong, Thailand, Nigeria, and Brazil. More information about the IPLEC program is available at www.justice.gov/criminal-ccips/overseas-work.

How Can You Assist Law Enforcement?

Prosecutions of intellectual property crime often depend on cooperation between victims and law enforcement. Indeed, without information sharing from intellectual property rights holders, prosecutors can neither discern the trends that suggest the most effective overall enforcement strategies, nor meet the burden of proving an intellectual property offense in a specific case. In addition to the checklist of information that would be helpful to include when reporting a violation, the following seeks to provide guidance concerning the types of ongoing assistance that may be offered by victims of intellectual property crime to law enforcement authorities.

- ❑ **Identify Stolen Intellectual Property:** Just as in cases involving traditional theft, such as a burglary or shoplifting, victims of intellectual property crime may – and often must – assist law enforcement in the identification of stolen property. Thus, law enforcement may call upon a victim representative or expert to examine items obtained during an investigation to determine their origin or authenticity. In a copyright infringement or counterfeit trademark investigation, for example, an author or software company may be called upon to analyze CDs, DVDs, or other media that appear to be counterfeit, while a victim representative in a theft of trade secret case may be asked to review internal documents or computer source code, as well as public materials such as patents and scientific publications. Prosecutors may later seek fact and/or expert testimony from the victims at trial.

In certain investigations, law enforcement agents also may request a victim's presence during the execution of a search warrant to help the agents identify specific items to be seized. In those circumstances, the victim's activities will be strictly limited to those directed by supervising law enforcement agents.

- ❑ **Share the Results of Internal Investigations or Civil Lawsuits:** As with any suspected crime, victims may provide law enforcement with information gathered as a result of internal investigations into instances of intellectual property theft. In addition, unless a court has ordered otherwise, victims may generally provide law enforcement with any evidence or materials developed in civil intellectual property enforcement actions, including court pleadings, deposition testimony, documents, and written discovery responses.
- ❑ **Contributions of Funds, Property, or Services:** Donating funds, property, or services to federal law enforcement authorities can raise potential legal and ethical issues that must be addressed on a case-by-case basis. In general, federal law places limitations on contributions to law enforcement authorities.



REPORTING INTELLECTUAL PROPERTY CRIME

A Guide for Victims of Copyright Infringement, Trademark Counterfeiting, and Trade Secret Theft

Third Edition

Checklist for Reporting an Intellectual Property Crime

This checklist serves as a guide for the type of information that would be helpful for a victim or a victim's authorized representative to include when reporting an intellectual property violation to law enforcement. The checklist contains two sections: one intended for use in criminal copyright and trademark cases, and the other intended for use in criminal trade secret cases. We encourage victims to report suspected crimes to law enforcement as soon as possible, with as much of the below information as time and circumstances allow. Victims typically do not have a complete picture of the criminal conduct and related facts and circumstances when the crime is first discovered. Law enforcement agents conduct investigations to find the truth and have investigative tools that are unavailable to private citizens and businesses. *Please note that a victim's written statements—even emails to law enforcement agents—may be discoverable in subsequent litigation.*

Prosecutors and/or investigators may also use the checklist as a framework to gather information from victims. They can be adapted for use in other intellectual property offenses as well. Reviewing the checklist *before* an incident occurs may also help rights holders identify what type of information they should be generating on an ongoing basis to help protect their rights.

Criminal Copyright and Trademark Infringement

- ✓ Background / Contact Information
- ✓ Description of the Intellectual Property (IP)
- ✓ Description of the Suspected IP Crime
- ✓ Origin and Entry (If Applicable)
- ✓ Possible Suspects
- ✓ Internet Involvement
- ✓ Civil Enforcement Proceedings

Criminal Trade Secret Offenses

- ✓ Note on Confidentiality
- ✓ Background / Contact Information
- ✓ Description of the Trade Secret
- ✓ Measures Taken to Protect the Physical Trade Secret Location
- ✓ Confidentiality and Non-Disclosure Agreements
- ✓ Electronically-Stored Trade Secrets
- ✓ Document Controls
- ✓ Employee Controls
- ✓ Description of the Trade Secret's Misappropriation
- ✓ Civil Enforcement Proceedings

Criminal Copyright and Trademark Infringement

1. Background and Contact Information

- Victim's Name:
- Primary Address:
- Nature of Business:
- Primary Contact:
- Work Phone:
- Mobile Phone:
- E-mail:
- Fax:
- In addition to primary contact listed above, please be prepared to provide the names, titles and contact information of all people with knowledge of information requested below.

2. Description of the Intellectual Property

- Describe the copyrighted material or trademark/service mark/certification mark (*e.g.*, title of copyrighted work, identity of logo), including any factors that make its infringement especially problematic (*e.g.*, threats to public health and safety, pre-release piracy).
- Is the work or mark registered with the U.S. Copyright Office or on the principal register of the U.S. Patent and Trademark Office?¹ ___ YES ___ NO

If yes, please provide the following:

- Registration Date:
- Registration Number:

If no, state if and when you intend to register:

- Do you have a certified copy of the certificate of registration? ___ YES ___ NO

¹ Registered trademarks can be found through the U.S. Patent & Trademark Office's searchable database at: tess2.uspto.gov

- Is the work or mark recorded with U.S. Customs and Border Protection (CBP)?²
___ YES ___ NO

If yes, please provide the following:

- Recordation Date:
- Recordation Number:

- What is the approximate retail value of the infringed work, good, or service?
- Has the work or mark been the subject of a previous civil or criminal enforcement action? If so, please provide a general description as well as the case name, case number, and name of court.

3. Description of the Intellectual Property Crime

- Describe how the theft or counterfeiting was discovered.
- Do you have any examination reports of the infringing or counterfeit goods?
___ YES ___ NO

If yes, please provide those reports to law enforcement. Please also provide a photograph or sample of the goods, if possible.

- Describe the type of infringement (*e.g.*, manufacture, reproduction, import, export, distribution).
- Describe the scope of the infringing operation, including the following information:
- Estimated quantity of illegal distribution:
 - Estimated value of illegal distribution:
 - Estimated time period of illegal distribution:
 - Is the illegal distribution national or international? Which states and/or countries?

² IP rights holders can apply online at apps.cbp.gov/e-recordations/ to record their trademarks and copyrights with CBP to protect against the importation of infringing products.

- Identify where the infringement or counterfeiting occurred, and describe the location.

4. Origin and Entry (If Applicable)

- Identify the country of origin of the infringing item.
- Identify the date, location, and mode of entry into the United States.
- Identify the names of shippers and Harmonized Tariff Schedule designation and provide any other applicable shipping or customs information.

5. Possible Suspects

- Identify the name(s) or location(s) of all possible suspects, including the following information:
 - Name:
 - Phone number:
 - E-mail address:
 - Physical address:
 - Current employer, if known:
 - Any other identifiers:
 - Reason for suspicion:

6. Internet Involvement

- If the distribution of infringing or counterfeit goods involves the Internet, identify the following:
 - How the Internet is involved (*e.g.*, websites, FTP, mail, chat rooms):
 - Relevant Internet address, including any affiliate websites (domain name, URL, IP address, e-mail):
 - Login or password for website:
 - Operators of website, if known:
 - Location of the servers and website host:
 - Country where domain name is registered:

- Has the rights holder sent a cease and desist notice to the website?
___ YES ___ NO

If yes, please provide the following:

- Date of notice:
- Do you have a copy of the notice? ___ YES ___ NO

- If you have conducted an internal investigation into the theft or counterfeiting activities, please describe any evidence acquired and submit, if possible, any investigative reports.

7. Civil Enforcement Proceedings

- Have you ever received counterfeit goods from the target listed above?
___ YES ___ NO

- If yes, did you place the target on notice that the goods received were counterfeit?

- Has a civil enforcement action been filed against the suspects identified above?
___ YES ___ NO

If yes, identify the following:

- Name of court and case number:
- Date of filing:
- Names of attorneys:
- Status of case:

If no, please state whether a civil action contemplated, what type and when.

- Have you contacted any other government agencies about this incident?

If yes, identify the agency contacted.

- Please provide any information concerning the suspected crime not described above that you believe might assist law enforcement.

Trade Secret Offenses

Note on Confidentiality: Federal law provides that courts “shall enter such orders and take such action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws.” 18 U.S.C. § 1835. Prosecutors generally will use protective orders and other appropriate measures to vigorously protect trade secrets during investigation and prosecution. See Levine & Flowers, [How Prosecutors Protect Trade Secrets](#), 38 Am. J. Trial Advoc. 461 (2014-2015).

1. Background and Contact Information

- Victim’s Name:
- Primary Address:
- Nature of Business:
- Primary Contact:
- Work Phone:
- Mobile Phone:
- E-mail:
- Fax:

- In addition to primary contact listed above, please be prepared to provide the names, titles and contact information of all people with knowledge of information requested below.

2. Description of the Trade Secret

- Generally describe the trade secret (*e.g.*, source code, formula, technology, process, device), and explain how that information differs from that disclosed within any issued patents and/or published patent applications.

- Provide an estimated value of the trade secret using one or more of the methods listed below:

Estimated Value	Method
	Cost to develop the trade secret
	Acquisition cost (include date / source of acquisition)
	Fair market value if sold / licensed

3. Measures Taken to Protect the Physical Trade Secret Location

Note: While the questions below address some common measures that rights holders may take to protect IP, there is no legal requirement that rights holders take all or even most of these particular measures. Whether a rights holder has taken “reasonable measures” to protect its IP is a context-specific determination that must be made on a case-by-case basis.

- Describe the company’s general security practices concerning entry to and moving within its premises, such as fencing the perimeter of the premises, visitor control systems, using alarming or self-locking doors or security personnel.
- Describe any security measures the company has employed to prevent unauthorized viewing or access to the trade secret, such as locked storage facilities or “Authorized Personnel Only” signs at access points.
- Describe any protocol the company employs to keep track of employees accessing trade secret material such as sign in/out procedures for access to and return of trade secret materials.
- Are employees required to wear identification badges? ___YES ___ NO
- Does the company have a written security policy? ___YES ___NO

If yes, please provide the following information:

- Does the security policy address in any way protocols on handling confidential or proprietary information? ___YES ___NO
- How are employees advised of the security policy?
- Are employees required to sign a written acknowledgment of the security policy? ___YES ___NO
- How many employees have access to the trade secret?
- Was access to the trade secret limited to a “need to know” basis? ___YES ___NO

If yes, describe how “need to know” was maintained in any ways not identified elsewhere (*e.g.*, closed meetings, splitting tasks between employees and/or vendors to restrict knowledge):

4. Confidentiality and Non-Disclosure Agreements

- Does the company enter into confidentiality and non-disclosure agreements with employees and third parties concerning the trade secret? ___YES ___NO
- Has the company established and distributed written confidentiality policies to all employees? ___YES ___NO
- Does the company have a policy for advising company employees regarding the company’s trade secrets? ___YES ___NO

5. Electronically-Stored Trade Secrets

- If the trade secret is computer source code or other electronically-stored information, how is access regulated (*e.g.*, are employees given unique user names, passwords, and electronic storage space, and was the information encrypted)?
- If the company stores the trade secret on a computer network, is the network protected by a firewall? ___YES ___NO

Is remote access permitted into the computer network? ___YES ___NO

If yes, is a virtual private network utilized? ___YES ___NO

Is the trade secret maintained on a separate computer server? ___YES ___NO

Does the company prohibit employees from using unauthorized computer programs or unapproved peripherals, such as high capacity portable storage devices? ___YES ___NO

Does the company maintain electronic access records such as computer logs?
___YES ___NO

6. Document Controls

If the trade secret consists of documents, were they clearly marked "CONFIDENTIAL" or "PROPRIETARY"? ___YES ___NO

Describe the document control procedures employed by the company, such as limiting access and sign in/out policies.

Was there a written policy concerning document control procedures?
___YES ___NO

If yes, how were employees advised of it?

7. Employee Controls

Are new employees subject to a background investigation?
___YES ___NO

Does the company conduct regular training for employees concerning steps to safeguard trade secrets? ___YES ___NO

Does the company hold "exit interviews" to remind departing employees of their obligation not to disclose trade secrets?
___YES ___NO

8. Description of the Misappropriation of the Trade Secret

- Identify the name(s) or location(s) of all possible suspects, including the following information:
 - Name:
 - Phone number:
 - E-mail address:
 - Physical address:
 - Current employer, if known:
 - Any other identifiers:
 - Reason for suspicion:

- Describe how the misappropriation of the trade secret was discovered.

- Describe the type(s) of misappropriation (*e.g.*, stealing, copying, drawing, photographing, downloading, uploading, altering, destroying, transmitting, receiving).

- If known, was the trade secret stolen to benefit a third party, such as a competitor or another business? ___YES ___NO

If yes, identify that business and its location.

- Do you have any information that the trade secret was stolen to benefit a foreign government or instrumentality of a foreign government? ___YES ___NO

If yes, identify the foreign government or instrumentality and describe that information.

- If the suspect is a current or former employee, describe all confidentiality and non-disclosure agreements in effect.

- Identify any physical locations associated with the misappropriated trade secret, such as where it may be currently stored or used.

- If you have conducted an internal investigation into the misappropriation, please describe any evidence acquired and provide any investigative reports that you can.

9. Civil Enforcement Proceedings

- Has a civil enforcement action been filed against the suspects identified above?
___YES ___NO

If yes, please provide the following information:

- Name of court and case number:
- Date of filing:
- Names of attorneys:
- Status of case:

If no, please state whether a civil action contemplated, what type and when.

- Have you contacted any other government agencies about this incident?

If yes, identify the agency contacted.

- Please provide any information concerning the suspected crime not described above that you believe might assist law enforcement.

Additional Resources

- ❑ CCIPS Website: www.cybercrime.gov
- ❑ CCIPS Main Number: (202) 514-1026
- ❑ [Prosecuting Intellectual Property Crimes Manual](#) (available online at www.justice.gov/criminal/cybercrime/docs/prosecuting_ip_crimes_manual_2013.pdf)
- ❑ [Prosecuting Computer Crimes Manual](#) (available online at www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf)
- ❑ Levine & Flowers, [How Prosecutors Protect Trade Secrets](#), 38 Am. J. Trial Advoc. 461 (2014-2015) (available online at www.justice.gov/criminal-ccips/file/640271/download)
- ❑ [Best Practices for Victim Response and Reporting of Cyber Incidents](#) (available online at www.justice.gov/criminal-ccips/file/1096971/download)
- ❑ [Arranging a Speaker from CCIPS](#) (available online at www.justice.gov/criminal-ccips/arranging-speakers)