WO

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Contractor Management Services LLC,

Plaintiff,

v.

Para Incorporated, et al.,

Defendants.

No. CV-25-01645-PHX-DWL

ORDER

This is a lawsuit between two "direct competitors," Contractor Management Services, LLC d/b/a Openforce ("Openforce") and Para, Inc. d/b/a GigSafe ("GigSafe"), in the contractor management software industry. (Doc. 1 ¶ 3.) In broad strokes, Openforce alleges that GigSafe and its CEO, Defendant David Pickerell, "feigned interest in a potential corporate transaction" in 2023, which resulted in the parties executing a non-disclosure agreement and then meeting in Arizona to exchange various categories of sensitive business information, and that GigSafe and Pickerell then "hacked into Openforce's systems, pilfered Openforce's trade secrets, and used that information to steal Openforce's customers." (*Id.* ¶¶ 1-3.) Based on those allegations, Openforce asserts claims against Pickerell and/or GigSafe for (1) misappropriation of trade secrets under the federal Defend Trade Secrets Act ("DTSA"); (2) misappropriation of trade secrets under the Arizona Uniform Trade Secrets Act ("AUTSA"); (3) tortious interference with contract; (4) tortious interference with business expectancy; (5) fraudulent misrepresentation; (6) fraudulent inducement of the non-disclosure agreement; (7) breach of the non-disclosure agreement; (8) unfair competition; and (9) unjust enrichment. (*Id.* ¶¶ 47-123.)

Now pending before the Court are GigSafe's and Pickerell's motions to dismiss. (Docs. 12, 13.) Those motions are fully briefed (Docs. 15, 16, 25, 26), and no party requested oral argument. For the reasons that follow, each motion is granted in part and denied in part.

BACKGROUND

I. Relevant Factual Allegations

The following relevant factual allegations are taken from the complaint (Doc. 1) and the mutual non-disclosure agreement (hereinafter, "MNDA") (Doc. 1-1).

A. **The Parties**

"Openforce is a Nevada limited liability company with its principal place of business in Scottsdale, Arizona." (Doc. 1 ¶ 8.) Openforce is "an industry leader in contractor management software that helps contracting companies manage their independent contractor vendor relationships and comply with labor regulations and assists independent contractors with managing their businesses." (*Id.* at 1.)

"Para is a Delaware corporation with . . . its principal place of business in San Francisco, California. It currently operates under the trade name GigSafe." (*Id.* ¶ 9.)

Pickerell "is a citizen of the State of Texas." (*Id.* ¶ 10.) Pickerell is the "founder and CEO" of "Para, now known as GigSafe." (*Id.* ¶ 1.)

B. **Openforce's Software And Trade Secrets**

"For over twenty years, Openforce has offered software-enabled solutions that serve contracting companies utilizing independent contractor workforces and independent contractors." (*Id.* ¶ 13.) Openforce's platform "covers all aspects of independent contractor management, including onboarding, regulatory compliance, risk management, rate negotiation, insurance, invoicing and settlement processing." (*Id.*)

"In its software deployment process, Openforce develops with its clients a workflow 'blueprint' and offers each of its clients a customizable Workflow Designer. This proprietary software tool allows companies to tailor their processes for on-boarding (or 'enrolling') new independent contractors." (*Id.* ¶ 14.) "These workflows and the materials contained in them (often called a blueprint) are a critical component of Openforce's offerings." (*Id.*)

Openforce's "customer workflows go hand-in-hand with Openforce's Contractor Management Platform, Manage (formerly IC Manage). Through Manage, Openforce's customers can streamline key aspects of their relationship with their independent contractors in ways that Openforce has fine-tuned over decades." (*Id.* ¶ 15.)

"Openforce has spent decades and invested many millions of dollars into the research and development of its software systems, including Manage, the Workflow Designer, and related enrollment offerings," and Openforce continuously works to "improve its offerings." (*Id.* ¶ 16.) As a result, Openforce has received several industry awards. (*Id.*)

"Openforce's continued success . . . depends on the intellectual property underlying its platform, which Openforce goes to great lengths to protect." (*Id.* ¶ 17.) That intellectual property includes Openforce's "Trade Secrets," which "span a wide variety of operations and business activity." (*Id.*) Those "Trade Secrets," as defined in the complaint, include:

> [1] customer preferences and requirements for enrolling independent contractors in their systems, which manifest in customers' tailored enrollment workflows that meet their own individual needs; . . . [2] the product that Openforce makes available to its customers, rendered in Manage and Openforce's other systems as, among other things, workflows containing the necessary steps that legitimate independent contractors take to enroll to do business with one of Openforce's customers[;] . . . [3] customer-specific pricing; [4] the customer's terms of engagement; [5] customer onboarding requirements; [6] workflow-development records, processes, and procedures; [7] strategies for insurance and regulatory compliance regarding the independent-contractor relationship; [8] process checks for verifying enrollees' identities and background information; [9] company/contractor agreements; [10] contractor/Openforce agreements; [11] independent contractor decision documentation; [12] insurance plan structures and their underlying forms; [13] contractor payment processes and forms; . . . [14] state-by-state variations regarding the above[;] . . . [15] Openforce's best practices and strategies for working with independent contractors,

> manifested throughout the Manage software, which includes specific processes for regulatory compliance, onboarding, recruiting, and benefits[;] . . . [16] the technological information that enable Openforce's industry-leading platforms, including functionalities, schematics, and diagrams of Openforce's software systems, including (a) Workflow Designer, as well as the resulting selection and arrangement of workflows it makes available to its customers, (b) Manage, and (c) Openforce's tailored and non-public administrative interfaces available only to clients with the necessary login credentials to access them[;] . . . [and] [17] the trial and error (both positive and negative) that Openforce undertook to create these trade secrets. All of these trade secret and confidential information described in this paragraph (collectively, the "Trade Secrets") are related to products or services that Openforce uses in, or intends to use in, interstate or foreign commerce . . . including Workflow Designer and Manage.

(*Id.,* brackets added.)

"Openforce's Trade Secrets derive considerable value from not being publicly known outside of Openforce," and "[t]hey derive independent economic value, actual and potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from their disclosure or use." (*Id.* ¶ 18.) To that end, "Openforce takes reasonable steps to protect its Trade Secrets from disclosure," including by, among other things, "limit[ing] access to the Trade Secrets through actions and procedures designed to prevent any unauthorized use or disclosure." (*Id.* ¶¶ 19-20.) For example, "[w]hen disclosing any Trade Secrets to third parties like customers and their independent contractors, Openforce requires these third parties to execute agreements with strict provisions preventing any unauthorized use or disclosure of any Openforce Trade Secrets," and "Openforce uses a unique, customer-specific activation code that Openforce provides to each of its customers to restrict the ability of a real independent contractor to access" Openforce's systems. (*Id.* ¶ 22.)

C. **GigSafe And GigSafe's Plan**

In 2020, Pickerell started Para, which "advertised an app for gig-economy workers, like delivery drivers, that purported to provide price transparency and a one-stop shop for managing work they performed for gig-economy companies like DoorDash and Uber."

(*Id.* ¶¶ 2, 23.) According to the complaint, "Para's app suffered from a major problem—it depended on Para unlawfully exploiting data from these gig-economy companies," which led to steps taken by companies like DoorDash and Uber to "halt Para's unlawful actions." (*Id.* ¶¶ 2, 23.) As a result, Para and Pickerell "g[ave] up on this particular business model" and instead "hatch[ed] a new conspiracy: rebrand Para as GigSafe, hack into Openforce's systems, steal its trade secrets and confidential information, and build a copycat platform to lure away Openforce's customers." (*Id.* ¶ 2.)

"Given Openforce's role as an industry leader in the contractor management space (an industry adjacent to the one occupied by DoorDash and Uber), Openforce was soon in Para's crosshairs." (*Id.* ¶ 24.) In June 2022, "Defendants put their plan into action . . . when Para employee Jimmy Thompson created an Openforce account posing as an independent contractor . . . with the intention of infiltrating Openforce's system, so that they could learn how Openforce operates and create a competing company." (*Id.*)

"The plan did not get far at first" because "Openforce restricts access to its on-boarding and enrollment platform . . . by limiting access to the enrollment platform to those with a customer-specific activation code." (*Id.* ¶ 25.) "Use of these codes and access to these systems is authorized only by actual independent contractors seeking work with Openforce's customers," and "[u]sing activation codes to access particularized workflows of any customer for any other purpose . . . is forbidden by an end user license agreement." (*Id.*)

Next, in April 2023, Para and Pickerell, in furtherance of their alleged plan, "first got in touch with Openforce" at "the Express Carrier's Association conference." (*Id.* ¶ 26.) "Unaware of Para's problematic past and its ploy" to steal Openforce's trade secrets, "Openforce stayed in touch with Para throughout that summer." (*Id.*)

D. The In-Person Arizona Meeting And The MNDA

Sometime in 2023, and "[i]n pursuit of this scheme, . . . Para and [Pickerell] feigned interest in a potential corporate transaction with Openforce." (*Id.* ¶ 3.) In order "[t]o solicit Openforce's confidential information, [Pickerell] claimed that Para needed substantive, detailed information about Openforce's business model, competitive strategies, and clients to better evaluate the contemplated Openforce-Para business transaction." (*Id.*)

Ultimately, "Openforce . . . arranged an in-person meeting in October 2023 [in Arizona] with Openforce's CEO, Chairman of the Board, and CTO to discuss next steps for a potential corporate transaction." (*Id.* ¶ 26.) "Before the October 2023 meeting, Openforce required Para to execute the MNDA, as is its practice." (*Id.* ¶ 27.) The MNDA was executed by both parties on September 7, 2023. (Doc. 1-1 at 3.)[1] The MNDA "provided that sensitive, confidential information would be shared by both parties to allow them to evaluate a potential business relationship." (Doc. 1 ¶ 27.)

The MNDA contains several provisions relevant to the parties' dismissal arguments, excerpted here:

> **Definition of Confidential Information.** Each party (the "Disclosing Party") may during the term of this Agreement disclose, or permit access to, to the other party (the "Receiving Party"), certain non-public information, including, but not limited to, information regarding: systems, personal information, agreements, data, payment information, patents and patent applications; trade secrets; mask works, ideas, concepts, knowhow, techniques, sketches, drawings, works of authorship, models, inventions, processes, algorithms, software (in both source code and object code formats), and formulas related to each of the parties (and their respective affiliates), including information regarding experiments, developments, designs, specifications, customer lists, product plans, investors (or potential investors), employees, agents, contractual relationships, forecasts, sales, merchandising, and marketing plans; business and personal information of employees, customers, vendors, and independent contractors, including but not limited to personal identification information, payment information, and contracting information; and regardless of whether so marked or confirmed, any unannounced or non-public products or services of the Disclosing Party (including such products or services themselves), and including without limitation business models, methodologies, customer lists and financial information (collectively, "Confidential Information"). With respect to Confidential Information disclosed orally or in intangible format, the Receiving Party shall treat all such orally disclosed Confidential Information as confirmed Confidential Information.

[1] Pickerell did not sign on behalf of Para—instead, the Para signatory was Robert Fierro, Para's chief revenue officer. (Doc. 1-1 at 3.)

(Doc. 1-1 at 2 § 1(a).)

> **Protection**. Except as expressly permitted by this Agreement, the Receiving Party, and any of its affiliates, parents, subsidiaries, and their respective employees, vendors, agents, officers, directors, and owners shall not disclose the Confidential Information of the Disclosing Party and shall not use the Confidential Information of the Disclosing Party for any purpose other than expressly permitted by the Disclosing Party. Such prohibited uses of the Confidential Information include but are not limited to: (i) to compete directly or indirectly with the Disclosing Party; (ii) to develop products or services competitive with those of the Disclosing Party; or (iii) to assist any third party in any of the foregoing.

(*Id.* § 1(b).)

> **Return of Confidential Information**. At the discretion and direction of the Disclosing Party, the Receiving Party shall return, destroy, or erase all Confidential Information of the Disclosing Party in tangible form within 15 business days after the expiration or termination of this Agreement, and confirm in writing to the Disclosing Party the completion of such directive.

(*Id.* § 1(d).)

> **Non-Solicitation.** The Parties agree to support and protect each other's efforts in performance of this Agreement by refraining during the life of this Agreement plus six months from any direct or indirect contact or solicitation of any customers, employees or opportunities introduced to one Party by the other Party. This explicitly excludes any customers or opportunities the Parties have previously engaged with or been presented and any employees responding to a publicly posted job opening so long as such employee was not solicited.

(*Id.* at 3 § 2.)

> **Choice of Law and Jurisdiction.** This Agreement shall be subject to the laws of the State of Arizona, without reference to its conflicts of laws principles. Any dispute arising under this Agreement shall be subject to the exclusive jurisdiction of the State and Federal Courts located in Phoenix, Arizona, and the parties hereby submit to the personal jurisdiction of such courts.

(*Id.* § 5.)

"To date, no party has terminated the MNDA; it remains in effect." (Doc. 1 ¶ 30.)

Following the execution of the MNDA, "[d]iscussions between Openforce and Para continued," and "[d]uring September 2023, Openforce's Chief Product Officer and VP of Marketing and Partnerships met with [Pickerell] and Jessica DiGulio, a Para operations employee. Openforce shared an overview of Openforce's products and services." (*Id.* ¶ 31.)

Finally, in October 2023, "[a]t an in-person meeting in Arizona between both sides' leadership, including [Pickerell], . . . Openforce shared information about its business pursuant to [the MNDA], including its pricing strategy, operating mechanics, insurance offerings, three-legged stool strategy, strategies to mitigate labor misclassification risks when retaining independent contractors, and revenue models." (*Id.* ¶ 3. *See also id.* ¶ 32 ["At this meeting, and pursuant to the MNDA, Openforce shared detailed and confidential business plans, growth strategies, insurance information, and its revenue models."].)

According to the complaint, "these talks were only a front for [Pickerell's] and Para's ploy—to learn enough about Openforce so they could take Openforce's trade secrets to compete with Openforce through their rebranded venture, GigSafe." (*Id.* ¶ 3.) Indeed, the complaint alleges that Openforce later learned that "[w]hile Para was meeting with Openforce, [Pickerell] had already started rebranding Para as GigSafe" as early as September 2023. (*Id.* ¶ 3, 34.) And "less than two weeks" after the parties met in person, "Para told Openforce that it had no interest in proceeding." (*Id.* ¶ 33.)

E. **The Subsequent Hacking Of Openforce's Systems**

"Defendants' scheme did not end" with the October 2023 in-person meeting. (*Id.* ¶ 4.) Following that meeting, Pickerell and GigSafe "implemented the next step in their scheme, in which GigSafe employees created accounts with Openforce by masquerading as independent contractor drivers seeking work from Openforce's clients—just as they had attempted with [Thompson] in June of 2022." (*Id.* ¶ 36.) But unlike Thompson's unsuccessful attempt in 2022, "this time was different, because [Pickerell] was now armed with information learned from Openforce under the MNDA. As a result, . . . GigSafe and [Pickerell] knew how to get these employees 'inside' Openforce's systems by posing as independent contractors and procuring customer-specific activation codes. Once inside, the GigSafe actors could access Openforce's Trade Secrets in the form of its customer-specific workflows and, by implication, the underlying Workflow Designer that Openforce uses to build them." (*Id.*)

"Over the next year and a half . . ., GigSafe and [Pickerell] misused the activation codes for at least ten Openforce customers." (*Id.*) And "[s]ince November 2023, and continuing to this day, GigSafe's personnel have lied about their identities and intentions to access Openforce's software system, which has allowed Defendants to misappropriate more of Openforce's proprietary, customer-specific enrollment and workflow information, insurance offerings, payment plans, system mechanics, and client admin interface designs. Openforce's internal logs reflect that at least six different GigSafe employees on over 20 separate occasions improperly accessed Openforce's platform by misrepresenting themselves as would-be independent contractor drivers for at least ten Openforce clients." (*Id.* ¶ 4.)[2]

The complaint proceeds to outline examples of GigSafe employees hacking into Openforce's systems by posing as independent contractors. (*Id.* ¶¶ 37-38.) "None of the[se] GigSafe employees . . . ever performed the courier services, retail merchandising services, supply chain management services, or other services as independent contractors for Customers A-J through Openforce's platform." (*Id.* ¶ 39.) "Instead," those employees "purposefully misrepresented their identities and intentions, enrolling to improperly access, learn about, and then misuse Openforce's Trade Secrets to design a copycat competing system and provide similar offerings." (*Id.*) "Shortly after learning that GigSafe employees were improperly using and accessing its systems, Openforce terminated access to its systems for all known accounts of GigSafe personnel." (*Id.* ¶ 40.)

F. GigSafe's Poaching Of Openforce's Customers

Ultimately, "GigSafe used the ill-gotten information from their hacking into Customer A-J's workflows in an attempt to poach them—in violation of the MNDA's

[2] Those ten clients are identified in the complaint by pseudonyms: Customers A-J. (*Id.* ¶ 5.)

customer non-solicitation provision." (*Id.* ¶ 41.) In March 2024, GigSafe's Thompson "sent a letter to a potential Openforce customer, 'Customer K,' which attacked Openforce by name and said that the potential use of Openforce would likely 'cost[] you a king's ransom to pay and insure your drivers.'" (*Id.* ¶ 42.) The complaint alleges that "this letter to Customer K is only one example of similar letters that GigSafe sent to actual or potential Openforce's customers." (*Id.* ¶ 43.) At least Customers B, F, and H have terminated their relationships with Openforce and are now identified on GigSafe's website as GigSafe customers. (*Id.* ¶¶ 44-46.)

II. <u>Procedural Background</u>

On May 14, 2025, Openforce initiated this action. (Doc. 1.)

On June 30, 2025, Pickerell filed his motion to dismiss. (Doc. 12.) That motion is now fully briefed. (Docs. 15, 26.) On the same day, GigSafe filed its motion to dismiss. (Doc. 13.) That motion is now fully briefed. (Docs. 16, 25.)

DISCUSSION

I. <u>Pickerell's Motion to Dismiss</u>

The complaint asserts seven causes of action against Pickerell: (1) trade secret misappropriation under the DTSA; (2) trade secret misappropriation under the AUTSA; (3) tortious interference with contract; (4) tortious interference with business expectancy; (5) fraudulent inducement; (6) unfair competition; and (7) unjust enrichment. (Doc. 1.) Pickerell moves under Rule 12(b)(2) to dismiss all claims against him for lack of personal jurisdiction. (Doc. 12.)[3]

A. Legal Standard

A defendant may move to dismiss for lack of personal jurisdiction. Fed. R. Civ. P. 12(b)(2). "In opposing a defendant's motion to dismiss for lack of personal jurisdiction, the plaintiff bears the burden of establishing that jurisdiction is proper." *Ranza v. Nike, Inc.*, 793 F.3d 1059, 1068 (9th Cir. 2015) (citation omitted). "Where, as here, the

[3] Pickerell also incorporates by reference the dismissal arguments in GigSafe's motion to dismiss. (Doc. 12 at 16.) The Court addresses those arguments below in its discussion of GigSafe's motion.

defendant's motion is based on written materials rather than an evidentiary hearing, the plaintiff need only make a *prima facie* showing of jurisdictional facts to withstand the motion to dismiss." *Id.* (cleaned up).

When ruling on a motion to dismiss for lack of personal jurisdiction, "uncontroverted allegations must be taken as true, and conflicts between parties over statements contained in affidavits must be resolved in the plaintiff's favor," but a "plaintiff may not simply rest on the bare allegations of the complaint." *Id.* (cleaned up). The Court may also consider "deposition testimony and other evidence" outside of the pleadings to determine whether it has personal jurisdiction. *Omeluk v. Langsten Slip & Batbyggeri A/S*, 52 F.3d 267, 268 (9th Cir. 1995). *See also Lee v. Plex, Inc.*, 773 F. Supp. 3d 755, 769 (N.D. Cal. 2025) ("The Court may also consider declarations and other evidence outside the pleadings to determine whether it has personal jurisdiction.") (cleaned up); 1 Gensler, Federal Rules of Civil Procedure, Rules and Commentary, Rule 12 (2025) ("The plaintiff must supply specific facts in support of personal jurisdiction.").

"Federal courts ordinarily follow state law in determining the bounds of their jurisdiction over persons." *Morrill v. Scott Fin. Corp.*, 873 F.3d 1136, 1141 (9th Cir. 2017) (quoting *Daimler AG v. Bauman*, 571 U.S. 117, 125 (2014)). "Arizona law permits the exercise of personal jurisdiction to the extent permitted under the United States Constitution." *Id.* (citing Ariz. R. Civ. P. 4.2(a).) Accordingly, whether the Court has personal jurisdiction over Pickerell "is subject to the terms of the Due Process Clause of the Fourteenth Amendment." *Id.*

"Constitutional due process requires that defendants have certain minimum contacts with a forum state such that the maintenance of the suit does not offend traditional notions of fair play and substantial justice." *Id.* (cleaned up). Minimum contacts exist "if the defendant has continuous and systematic general business contacts with a forum state (general jurisdiction), or if the defendant has sufficient contacts arising from or related to specific transactions or activities in the forum state (specific jurisdiction)." *Id.* at 1142 (cleaned up).

Openforce does not contend that Pickerell is subject to general personal jurisdiction in Arizona. Thus, the Court must apply the Ninth Circuit's three-prong test to determine whether Pickerell has sufficient contacts with Arizona to be subject to specific personal jurisdiction: "(1) The non-resident must purposefully direct his activities or consummate some transaction with the forum or resident thereof; or perform some act by which he purposefully avails himself of the privilege of conducting activities in the forum, thereby invoking the benefits and protections of its laws; (2) the claim must be one which arises out of or relates to the defendant's forum-related activities; and (3) the exercise of jurisdiction must comport with fair play and substantial justice, i.e., it must be reasonable." *Id.* (citation omitted). "The plaintiff bears the burden of satisfying the first two prongs of the test." *Id.* (citation omitted). "If the plaintiff succeeds in satisfying both of the first two prongs, the burden then shifts to the defendant to 'present a compelling case' that the exercise of jurisdiction would not be reasonable." *Id.* (citation omitted).

B. **The Parties' Arguments**

Pickerell argues that he is "a Texas resident who attended a single meeting in Arizona with [Openforce]" and that "the only conduct in the Complaint that is tied to Arizona is [that] single meeting with Openforce that occurred in October 2023." (Doc. 12 at 1.) Pickerell argues that "Openforce attempts to create personal jurisdiction by baldly alleging that some sort of plan to access [Openforce's] systems was conceived in connection with that single 2023 meeting," but "Openforce does not allege that Pickerell used any of the information allegedly shared at the meeting to access Openforce's systems." (*Id.*) Pickerell further argues that "allegations arising from a single meeting would be insufficient to establish that [he] either purposefully directed his activities at Arizona or that the claims against him arise out of contacts with the state." (*Id.*) Pickerell further argues that Openforce's "attempts to establish jurisdiction through" the MNDA and Openforce's "own contacts with Arizona" must fail because "Pickerell is not a party to the" MNDA, and "a plaintiff's own contacts with the forum-state are irrelevant to the issue of personal jurisdiction over a defendant." (*Id.* at 2.) With respect to the MNDA, Pickerell emphasizes that “Openforce does not allege that the MNDA (which was not signed by Pickerell) was executed in Arizona. Nor does it allege that the misrepresentations purportedly made by Defendants to fraudulently induce Openforce to enter into the MDNA were made in Arizona.” (*Id.* at 8.) With respect to the meeting in Arizona, Pickerell emphasizes that “Openforce does not allege any facts tying the confidential and trade secret information supposedly shared at the Arizona meeting to Pickerell’s conduct following the meeting.” (*Id.* at 8-9.) Pickerell argues that “Defendants’ alleged conduct relates to the claimed unauthorized access of Openforce’s system by GigSafe employees through customer accounts with customer-specific activation codes,” but “[t]he Complaint makes no connection between the use of [those] customer activation codes and the Arizona meeting.” (*Id.* at 9.) Pickerell further argues that none of the causes of action asserted against him arise out of or relate to his contacts with Arizona because “all of the supposedly inappropriate access to Openforce’s systems occurred independent of [the in-person] meeting and no allegations even suggest that information at that meeting was used to gain the access to the systems in question.” (*Id.* at 10.) Finally, Pickerell argues that “even if the Court finds sufficient minimum contacts . . . , the exercise of personal jurisdiction offends traditional notions of fair play and substantial justice” because the seven factors used to evaluate reasonableness by the Ninth Circuit all weigh against the exercise of personal jurisdiction. (*Id.* at 13-16.)

In response, Openforce argues that “[d]espite [Pickerell’s] best attempts to pull apart the breach of the [MNDA] and his (and GigSafe’s) improper access to Openforce’s systems, the two are entwined” because “[b]oth forms of misconduct are part of the same overarching scheme to misappropriate Openforce’s trade secrets and confidential information to build a copycat company.” (Doc. 15 at 1.) Openforce emphasizes that during the October 2023 meeting in Arizona, “Openforce shared with [Pickerell] and his team key confidential and trade secret information, including its pricing strategy, operating mechanics, insurance offerings, three-legged stool strategy, strategies to mitigate labor misclassification risks, and revenue models” and that the complaint “alleges that GigSafe’s misappropriation and wrongful conduct *included information disclosed at this meeting and under the MNDA*." (*Id.* at 3, emphasis added.) Applying the purposeful-direction test for specific personal jurisdiction, Openforce argues that Pickerell purposefully directed his activities at Arizona by "physically travel[ing] to Arizona to meet with Openforce under false pretenses of a corporate transaction to further his plot to misappropriate Openforce information," and that Pickerell "did so under the guise of a contract with an Arizona forum selection clause into which he caused GigSafe to enter." (*Id.* at 6.) Openforce next argues that Pickerell's actions were expressly aimed at Arizona because (1) he "caused [GigSafe] to enter into the MNDA and include in that NDA an Arizona forum selection clause"; (2) the "in-person meeting at Openforce's headquarters in Scottsdale, Arizona" is "central to the events giving rise to this dispute" and is "the linchpin of the misconduct alleged in the Complaint"; (3) he "caused GigSafe personnel to fraudulently enroll as independent contractors for Openforce customers who have substantial ties to Arizona";[4] (4) he personally "engaged in the cyberespionage" by posing as a contractor on Openforce's systems "just hours before Openforce filed the Complaint"; and (5) he "solicited business in Arizona" by building "GigSafe's platform to compete for [Openforce's] customer base, including targeting business with independent contractors based in Arizona." (*Id.* at 7-11). Openforce also argues the effects of Pickerell's actions were foreseeable in Arizona because "[b]ut for [Pickerell's] contacts with Arizona, he would not have caused Openforce economic injury in Arizona." (*Id.* at 11-12.) Last, Openforce argues that under the Ninth Circuit's seven-factor test for reasonableness, Pickerell has failed to meet his burden. (*Id.* at 13-16.)

In reply, Pickerell largely reiterates his arguments from his motion. Among other things, Pickerell argues that "[a]ttendance at a single meeting in the forum with an Arizona-based company is insufficient to establish express aiming." (Doc. 26 at 4.) He also argues that Openforce's contention in its response that the October 2023 Arizona meeting was

[4] In support of this argument, Openforce provides a declaration from its Chief Technology Officer that purports to illustrate the Arizona connections of several of its customers. (Doc. 15-1.)

"central to the events giving rise to the dispute" (Doc. 15 at 7) is contrary to "what Openforce asserted in its response to the GigSafe Motion to Dismiss" (Doc. 26 at 5). Pickerell reiterates that the in-person meeting in Arizona could have happened anywhere and "does not establish that Defendants were expressly aiming their conduct at Arizona." (*Id.*) Pickerell also argues that Openforce cannot rely on the Arizona contacts of its own customers to support the exercise of personal jurisdiction and, at any rate, Openforce's customers' contacts with Arizona are "limited." (*Id.* at 7-10.) Pickerell also reiterates that "Openforce again fails to explain how Defendants misappropriated information obtained from the meeting [in Arizona] or how information learned at the meeting allowed Pickerell to access Openforce's platform" and that "Openforce admits that information learned at the meeting is unrelated to the alleged hacking supporting the tort claims." (*Id.* at 11.)

C. **Analysis**

Because Openforce's claims against Pickerell are all tort or tort-like causes of action,[5] both parties assume that the purposeful-direction test—sometimes known as the *Calder* effects test—governs the analysis here. (Doc. 12 at 6; Doc. 15 at 6; Doc. 26 at 3.) This assumption is understandable, as courts "generally apply the purposeful availment test when the underlying claims arise from a contract, and the purposeful direction test when they arise from alleged tortious conduct." *Morrill*, 873 F.3d at 1142. Nevertheless, the Ninth Circuit in *Freestream Aircraft (Bermuda) Ltd. v. Aero L. Grp.*, 905 F.3d 597 (9th Cir. 2018), clarified that a district court's application of the *Calder* effects test is "misplaced . . . for conduct that takes place inside the forum state." *Id.* at 603-04. Although "a purposeful direction analysis naturally applies in suits sounding in tort where the tort was committed outside the forum state," Ninth Circuit "jurisprudence makes clear that [*Paccar Int'l, Inc. v. Com. Bank of Kuwait, S.A.K.*, 757 F.2d 1058 (9th Cir. 1985)], not *Calder*, is the proper starting place where an intentional tort is committed within the forum state." *Id.* at 605-06. Under *Paccar*, there exists a "well-settled understanding that the

[5] Count Nine is a claim for unjust enrichment, and "unjust enrichment is an equitable claim for relief and not a tort." *Healixa Inc. v. Int'l Monetary*, 2025 WL 4058862, *5 (C.D. Cal. 2025).

commission of a tort within the forum state usually supports the exercise of personal jurisdiction." *Freestream Aircraft*, 905 F.3d at 606. Thus, district courts within the Ninth Circuit, relying on *Freestream Aircraft*, have declined to apply the *Calder* effects test where even "part of the alleged tort occurred in" the forum state. *Martensen v. Koch*, 942 F. Supp. 2d 983, 994 (N.D. Cal. 2013), on reconsideration in part, 2013 WL 4734000 (N.D. Cal. 2013). *See also Williams v. Pac. Sunwear of Cal. LLC*, 2024 WL 4626541, *4 (D. Ariz. 2024) ("Defendant skips a crucial step in its jurisdictional analysis. As will be explained below, the purposeful direction test only applies to tortious conduct that occurs outside the forum state. It does not govern tortious conduct that takes place inside the forum."); *Climax Portble Mach. Tools, Inc. v. Trawema GmbH*, 2020 WL 1304487, *3 (D. Or. 2020) ("Given the Ninth Circuit's guidance in *Freestream Aircraft*, the threshold question is whether part of the alleged tortious conduct occurred in [the forum state]. If so, the *Paccar* purposeful availment analysis is appropriate, and not the effects test under *Calder*.").

Under *Paccar*, if Pickerell is alleged to have committed an intentional tort (or part of the alleged tortious conduct) during the October 2023 in-person meeting in Arizona, then "the first two prongs of the minimum contacts test are satisfied" and the Court can move to the fair-play-and-substantial-justice prong. *Freestream Aircraft*, 905 F.3d at 603-04 (cleaned up). *See also Williams*, 2024 WL 4626541 at *5 ("Absent extraordinary circumstances such as those present in *Morrill*, if a defendant engages in tortious conduct inside the forum state, then the first two prongs of the minimum contacts test are automatically met. In such instances, there is no need to conduct a purposeful direction analysis. A court would proceed straight to the third prong, under which an objecting defendant must affirmatively demonstrate that the maintenance of jurisdiction offends fair play and substantial justice.").[6]

[6] The "extraordinary circumstances" in *Morrill* were that the defendants there were "*required* . . . to conduct activity in Arizona" because of litigation obligations and "thus were not in the forum state of their own volition." *Williams*, 2024 WL 4626541 at *5 (citation omitted). "By contrast," where a defendant "*voluntarily* travel[s]" to the forum state, *Paccar* applies. *Id.* (citation omitted). Here, there is no allegation that Pickerell's

At least some of Openforce's claims against Pickerell are founded on the allegation that Pickerell improperly obtained trade secrets and other confidential information from Openforce during the October 2023 in-person meeting in Arizona. For example, the complaint alleges that "[a]t an in-person meeting between both sides' leadership, including [Pickerell], in October 2023, Openforce shared information about its business pursuant to a non-disclosure agreement, including its price strategy, operating mechanics, insurance offerings, three-legged stool strategy, strategies to mitigate labor misclassification risks when retaining independent contractors, and revenue models." (Doc. 1 ¶ 3. *See also id.* ¶ 32 ["[A]t an in-person meeting on October 19, 2023 in Scottsdale, Arizona . . . Openforce shared detailed and confidential business plans, growth strategies, insurance information, and its revenue models."].) Several of the categories of information disclosed at that meeting overlap with the categories of "Trade Secrets" defined in paragraph 17 of the complaint. (*Id.* ¶ 17 [defining "Trade Secrets" as, among other things, "customer-specific pricing," "strategies for insurance and regulatory compliance," "insurance plan structures and their underlying forms," and "Openforce's best practices and strategies for working with independent contractors"].) And the categories of information disclosed at the in-person meeting also overlap with the allegedly misappropriated "Trade Secrets" underlying Counts One and Two. (*See, e.g.*, *id.* ¶ 48 [Count One: defining Trade Secrets as, among other things, "documents that reveal Openforce's . . . on-boarding processes, business operations, and compliance strategies; and information related to Openforce's insurance plans, compliance strategies, and payroll offerings"]; *id.* ¶ 58 [Count Two: same].) The complaint also alleges that "[t]he events and omissions in [Arizona] further include . . . Defendants' actions to . . . misappropriate the confidential and trade secret information of Openforce . . . *including by soliciting this information at the October 2023 meeting with Openforce that took place in [Arizona]*." (*Id.* ¶ 12, emphasis added.) Likewise, the unfair competition claim in Count Eight is premised in part on the allegation that "Pickerell . . . improperly accessed and misused Openforce's confidential information in the ways

decision to attend the in-person meeting in Arizona was involuntary.

described above and incorporated here, including by . . . entering into the MNDA in order to obtain Openforce's Trade Secrets and confidential information, despite having no intention of a potential corporate transaction with Openforce; . . . retaining those materials, and . . . using them in direct competition with Openforce." (Doc. 1 ¶ 113.) Because the complaint alleges that Openforce shared confidential information during the in-person meeting in Arizona "pursuant to" the MNDA (*id.* ¶ 3), it is plausible to infer that Count Eight is also premised, at least in part, on Pickerell's accessing of Openforce's confidential information during the in-person meeting in Arizona.

Pickerell disagrees that the complaint alleges that he misused whatever confidential information and trade secrets he may have obtained during the October 2023 meeting, arguing that "Openforce does not allege any facts tying the confidential and trade secret information supposedly shared at the Arizona meeting to Pickerell's conduct following the meeting. Defendants' alleged conduct relates to the claimed unauthorized access of Openforce's system by GigSafe employees through customer accounts with customer-specific activation codes. . . . The Complaint makes no connection between the use of customer activation codes and the Arizona meeting." (Doc. 12 at 8-9.) But Pickerell's reading of the complaint is too narrow. Although the complaint alleges that "information learned from Openforce" during the in-person meeting gave Pickerell and GigSafe the know-how "to get [GigSafe's] employees 'inside' Openforce's systems by posing as independent contractors and procuring customer-specific activation codes" (Doc. 1 ¶ 36), the complaint also alleges that the trade secret and other confidential information obtained by Pickerell during the in-person meeting was *itself* improperly accessed and therefore misappropriated. This reading of the complaint is confirmed by Openforce's briefing, which—contrary to Pickerell and GigSafe's protestations that Openforce has somehow abandoned its initially pleaded theory of liability (*see, e.g.*, Doc. 26 at 5)—explains that these are two separate, albeit "entwined" examples of accessing Openforce's information as part of an "overarching scheme to misappropriate Openforce's trade secrets." (Doc. 15 at 1; Doc. 16 at 1, 7, 17.)

The complaint also alleges that Pickerell acquired Openforce's trade secrets *through improper means* in Arizona. For example, the complaint alleges that the "talks" at the "in-person meeting in Arizona" were "only a front for [Pickerell's] and Para's ploy—to learn enough about Openforce so they could take Openforce's trade secrets to compete with Openforce through their rebranded venture, GigSafe." (Doc. 1 ¶ 3.) The complaint also alleges that GigSafe and Pickerell "feigned interest in a potential corporate transaction with Openforce" in order to obtain this information during the in-person meeting. (*Id.*)

Both the DTSA and AUTSA define "misappropriation" as including the acquisition of a trade secret by "improper means." 18 U.S.C. § 1839(5); A.R.S. § 44-401(2). Both statutes further define "improper means" as "includ[ing] 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. § 1939(6)(A); A.R.S. § 44-401(1). Here, the complaint plausibly alleges that Pickerell acquired Openforce's trade secrets and other confidential information during the in-person meeting in Arizona through improper means—i.e., by feigning interest in a corporate transaction with Openforce with the intent to use Openforce's trade secrets to compete with Openforce. Therefore, the complaint plausibly alleges that at least part of the allegedly tortious conduct occurred in the forum, and thus the *Paccar* test (and not the *Calder* effects test) applies.

Given this backdrop, the case for exercising personal jurisdiction over Pickerell in Arizona with respect to Counts One, Two, and Eight is, if anything, even stronger than the case for exercising personal jurisdiction that was present in *Climax Portble Machine Tools*. There, the plaintiff alleged that two former employees ("Individual Defendants") and their new employer ("Trawema") "misappropriated Plaintiff's confidential information and used it to the detriment of Plaintiff." 2020 WL 1304487 at *3. "Specifically, Plaintiff allege[d] that the Individual Defendants, while still employed by Plaintiff, downloaded confidential files from Plaintiff's computer server in Oregon and otherwise obtained confidential design files from Plaintiff's headquarters in Oregon so that Trawema could manufacture copies of two of Plaintiff's products and sell them in competition with Plaintiff." *Id.* Notably, it does not appear that the Individual Defendants actually set foot in Oregon—instead, while in Germany, they accessed servers they knew to be present in Oregon. *Id.* at *4. Nevertheless, the district court concluded that the Individual Defendants were subject to personal jurisdiction in Oregon in light of *Freestream Aircraft* and *Paccar*: "The question for jurisdiction purposes . . . is whether that alleged act [of obtaining the trade secrets] constituted committing a tort 'in Oregon' or the tort of misappropriation in Germany, with an effect in Oregon. The Court finds that the better analysis is that it was a tort that was at least in part committed in Oregon . . . ." *Id.* The court noted that "[o]ther courts also have found that acquisition of trade secrets from a server in the forum state with knowledge of its location, or other intentional and knowing improper use of a computer server in the forum state, creates enough minimum contacts to support personal jurisdiction, without analyzing the effects test." *Id.* at *5 (citations omitted). Here, of course, the allegation is not merely that Pickerell improperly obtained trade secrets from a server that was located in Arizona—indeed, there are no allegations regarding where Openforce's servers are located. Instead, Pickerell is alleged to have physically traveled to Arizona for the purpose of improperly obtaining those trade secrets in-person. The Court is hard-pressed to see how such conduct would not qualify, at least in part, as "the commission of a tort within a forum state." *Freestream Aircraft*, 905 F.3d at 606.

Other cases support that the jurisdictional analysis turns on whether the defendant acquired the trade secrets in the forum state through improper means. For example, in *Gold Medal Prods. Co. v. Bell Flavors & Fragrances, Inc.*, 2017 WL 1365798 (S.D. Ohio 2017), the plaintiff, Gold Medal, argued that the district court could "assert jurisdiction over Bell Flavors because its employee, Sunderhaus, worked for Gold Medal in Ohio, Sunderhaus obtained Gold Medal's trade secrets in Ohio, and Bell Flavors instructed Sundershaus to use or disclose those trade secrets for its benefit knowing that Gold Medal would suffer tortious injury in Ohio." *Id.* at *6. The court disagreed, in part because "Gold Medal ha[d] not alleged that Sunderhaus took wrongful acts in Ohio which Bell Flavors could have ratified. Sunderhaus obtained Gold Medal's trade secrets lawfully during the normal course of his employment for the company." *Id.* at *6. The court drew an analogy to *Drayton Enters., LLC v. Dunker*, 142 F. Supp. 2d 1177 (D.N.D. 2001), where the district court declined to exercise personal jurisdiction over a company that had hired a former employee of the plaintiff "because [the former employee] had obtained the trade secret information by legitimate means in North Dakota before moving out of the state." *Gold Medal Prods.*, 2017 WL 1365798 at *7. Ultimately, the *Gold Medal* court held that it could not exercise personal jurisdiction over Bell Flavors in part because "Sunderhaus acquired the trade secret information in Ohio by legitimate means and only is alleged to have taken wrongful acts outside of the forum state more than one year later." *Id.* at *8. *See also Mitek Corp. v. Diedrich*, 2018 WL 5078385, *6 (N.D. Ill. 2018) ("Although Diedrich acquired Mitek's trade secrets in Illinois and Arizona, he did so in the course of a legitimate employment relationship and pursuant to his job duties. He later (allegedly) misappropriated those trade secrets to AFCO's benefit by soliciting a DSP amplifier from EVR, but Mitek does not claim that either party to that conversation was in Illinois at the time. These alleged facts accordingly do not give rise to specific jurisdiction over AFCO in Illinois.") (cleaned up).

The pattern that emerges from this caselaw is that if a plaintiff alleges that a defendant acquired trade secret information from the plaintiff through improper means while physically present in the forum state, the first two minimum-contacts factors are met under the *Paccar* framework. Such is the case here.

It is of no moment that the aforementioned cases involved former employees who likely spent more time than just a single meeting in the forum. Although Pickerell seems to suggest that attendance at a single meeting in the forum cannot establish specific personal jurisdiction (Doc. 12 at 1), Pickerell cites no authority in support of this supposed rule. If the tort itself (or at least a portion of the tort itself) was committed during a single meeting in the forum, that is sufficient to support to exercise of personal jurisdiction. *Freestream Aircraft*, 905 F.3d at 600 (holding that the defendant was subject to personal jurisdiction in Nevada based on a statement he made during a single trip to Nevada to attend a conference: "A defendant who travels to Nevada and commits an intentional tort there can be sued in that state, absent circumstances that would make such a suit unreasonable."). *Cf. RNS Servicing, LLC v. Spirit Constr. Servs., Inc.*, 2018 WL 3729326, *5 n.5 (N.D. Ill. 2018) ("Tak contends that a single meeting is insufficient to establish personal jurisdiction, but this leaves out the crux of the allegation that Tak intentionally came to Illinois and made false representations to an Illinois-based company. There is no bright-line numerical threshold of contacts necessary for personal jurisdiction; the question is simply whether the claims arise out of the defendant's contact with the forum state."); *Kingsley Cap. Mgmt., LLC v. Sly*, 820 F. Supp. 2d 1011, 1017-18 (D. Ariz. 2011) ("Without admitting any of these accusations, Cunningham says they fall short of activities purposefully directed at Arizona. He attended a single meeting at which Kingsley was an invited guest, and that meeting happened to be in Arizona. But Cunningham views the personal jurisdiction test too narrowly. Kingsley claims that the Oxygen investment was a scam perpetrated by various persons acting together, including Cunningham. Kingsley infers that the March 2008 investor meeting in Arizona was used, at least in part, to convince Kingsley to invest in a scam.").

Pickerell also seeks to draw parallels between this case and *E3 Innovation Inc. v. DCL Techs. Inc.*, 2021 WL 5741442 (D. Ariz. 2021), but *E3 Innovation* is distinguishable for several reasons. There, the Court applied the "effects test" in determining whether to exercise personal jurisdiction over three independent contractors of the plaintiffs who allegedly misappropriated the plaintiffs' confidential information. *Id.* at *6-7. In assessing the second element of the effects test—express aiming—the Court, quoting *Walden v. Fiore*, 571 U.S. 277, 285 (2014), was "guided by the principle that it 'must focus on the defendant's contacts with the forum state, not the defendant's contacts with a resident of the forum.'" *E3 Innovation*, 2021 WL 5741442 at *7. The *E3 Innovation* plaintiffs raised four theories of "express aiming," only one of which involved physical presence in Arizona. *Id.* at *8. As for that in-forum meeting, the Court noted that "Plaintiffs do not assert that [defendant's] dinner meeting . . . was related to, or in any way furthered, the tort of misappropriation of confidential information" and thus determined that the meeting was "not relevant to the 'express aiming' analysis." *Id.* Here, in contrast, Openforce expressly alleges that the in-person meeting in Arizona was related to, and furthered, the misappropriation of Openforce's trade secrets. More broadly, it does not appear that any part of the tortious conduct in *E3 Innovation* actually *occurred* in Arizona. Unlike in *Climax Portble Machine Tools*, the record in *E3 Innovation* reflected that "the alleged acts of misappropriation involved email accounts and cloud-based servers *not* located in Arizona." *E3 Innovation*, 2021 WL 5741442 at *9. These differences explain why the effects test was applicable in *E3 Innovation* but is inapplicable here.

Pickerell also places significant emphasis on language from *E3 Innovation* which, relying on *Walden*, stated:

> As in *Walden*, none of Blum's challenged conduct (*i.e.*, misappropriation of confidential information) has anything to do with Arizona itself. The misappropriation may have harmed an Arizona resident, but it would be error to impute E3's forum connections to Blum. That E3 is an Arizona business does not, on its own, establish that Blum expressly aimed his alleged conduct at Arizona because it does not relate to *Blum's* conduct. In the same vein, it is irrelevant for "express aiming" purposes that Blum's contractor relationship was negotiated in Arizona, that the confidential information was developed in Arizona and used to fulfill customer orders through Arizona channels, or that Blum received access to information via permissions granted by E3's Arizona office. This is because those facts are inextricably bound up with E3's location in Arizona. If, for example, E3 had been headquartered in California, none of these asserted contacts would have occurred in Arizona: the contractor relationship would have been negotiated in California, the confidential information would have been developed in California, and so on. None of these considerations suggest that Blum expressly aimed his misappropriation tort at Arizona, as opposed to whatever state happened to surround E3's headquarters.

Id. But again, the critical distinction here is that Pickerell is alleged to have reached out to Openforce to set up a meeting, which was held in Arizona, with the express purpose of improperly accessing Openforce's trade secrets and confidential information during that meeting. Thus, under *Paccar*, the first two elements of the minimum-contacts test are satisfied.

The inquiry does not end there, as the Court must still analyze whether the exercise of personal jurisdiction over Pickerell with respect to Counts One, Two, and Eight would comport with fair play and substantial justice, i.e. whether it would be reasonable. "In determining reasonableness, seven factors are considered: (1) the extent of a defendant's purposeful interjection; (2) the burden on the defendant in defending in the forum; (3) the extent of conflict with the sovereignty of the defendant's state; (4) the forum state's interest in adjudicating the dispute; (5) the most efficient judicial resolution of the controversy; (6) the importance of the forum to the plaintiff's interest in convenient and effective relief; and (7) the existence of an alternative forum." *Rio Props., Inc. v. Rio Int'l Interlink*, 284 F.3d 1007, 1021 (9th Cir. 2002). "As no single factor is dispositive, a court must balance all seven." *Id.*

As for the first and fourth factors, Pickerell essentially reiterates his arguments that his actions were not directed at Arizona and that Openforce's claims do not arise out of his Arizona contacts. But the Court has already determined that the complaint plausibly alleges that Pickerell attended the in-person meeting in Arizona with the purpose of improperly accessing Openforce's trade secrets and confidential information during that meeting. That is a significant purposeful interjection, and Arizona has an interest in adjudicating this dispute. The first and fourth factors thus weigh in Openforce's favor.

As for the second factor, the Court acknowledges that there is a burden on Pickerell, a Texas resident, to travel to Arizona. But as Openforce notes, it's hard to imagine how Pickerell can "credibly argue that litigating in Arizona imposes an undue burden when, as the CEO and key witness of GigSafe, he will be involved in the litigation there regardless." (Doc. 15 at 14.) The second factor is therefore, at best, neutral.

As for the third factor, Pickerell doesn't allege that any conflict exists between the laws of Arizona and Texas as to the claims at issue. To the contrary, he appears to argue under the seventh factor that Texas "recognizes similar causes of action." (Doc. 12 at 15.) Moreover, Pickerell's motion to dismiss incorporates by reference GigSafe's motion to dismiss, and GigSafe's motion applies Arizona law (not Texas law) to the various tort claims asserted here (Doc. 13). This factor therefore tips in Openforce's favor.

The fifth Factor, which "depends primarily on where the witnesses and the evidence are likely to be located," "is no longer weighed heavily given the modern advances in communication and transportation." *Freestream Aircraft*, 905 F.3d at 609 (cleaned up). At any rate, Openforce correctly notes that "Openforce's breach of contract claim against GigSafe will be in Arizona because of the forum selection clause," as will any "tort claims against GigSafe attendant to the MNDA claims," and it therefore "makes little sense to require parallel proceedings in two different states given the overlapping facts, parties, and core legal issues." (Doc. 15 at 15.) Therefore, this factor either tips slightly in Openforce's favor or is at best neutral.

As for the sixth factor, it is generally not given much weight, *Freestream Aircraft*, 905 F.3d at 609, so at best it tips slightly in favor of Openforce.

As for the seventh factor, Openforce "bear[s] the burden of proving the unavailability of an alternative forum," *id.*, and has not met that burden on this record. Thus, the seventh factor tips in favor of Pickerell.

On balance, Pickerell—who bears the ultimate burden on reasonableness—has not presented a compelling case that the exercise of personal jurisdiction over him with respect to Counts One, Two, and Eight would be unreasonable.

That leaves Openforce's claims against Pickerell in Counts Three (tortious interference with contract), Four (tortious interference with business expectancy), Six (fraudulent inducement), and Nine (unjust enrichment). Under Ninth Circuit law, "[i]f personal jurisdiction exists over one claim, but not others, the district court may exercise pendent personal jurisdiction over any remaining claims that arise out of the same 'common nucleus of operative facts' as the claim for which jurisdiction exists." *Picot v. Weston*, 780 F.3d 1206, 1211 (9th Cir. 2015) (citation omitted). *See generally Action Embroidery Corp. v. Atl. Embroidery, Inc.*, 368 F.3d 1174, 1180-81 (9th Cir. 2004) ("Many of our sister circuits have adopted the doctrine of 'pendent personal jurisdiction.' Under this doctrine, a court may assert pendent personal jurisdiction over a defendant with respect to a claim for which there is no independent basis of personal jurisdiction so long as it arises out of a common nucleus of operative facts with a claim in the same suit over which the court does have personal jurisdiction. . . . When a defendant must appear in a forum to defend against one claim, it is often reasonable to compel that defendant to answer other claims in the same suit arising out of a common nucleus of operative facts. We believe that judicial economy, avoidance of piecemeal litigation, and overall convenience of the parties is best served by adopting this doctrine."). Here, Counts Three, Four, Six, and Nine arise of the same common nucleus of operative fact as Counts One, Two, and Eight. The Court thus chooses, in its discretion, to exercise personal jurisdiction over Pickerell with respect to those claims, too. *Cf. Gigacloud Tech., Inc. v. Linon Home Decor Prods., Inc.*, 2025 WL 656653, *6 (C.D. Cal. 2025) (exercising pendent personal jurisdiction "over Defendants as to Plaintiffs' breach of contract, tortious interference of contract, tortious interference with economic advantage, and violation of California Unfair Competition Law claims" because "the Court has personal jurisdiction over Moving Defendants as to Plaintiffs' trade secrets misappropriation claim" and "Plaintiffs' trade secrets misappropriation claim and Plaintiff's remaining claims . . . arise out of a common nucleus of operative fact").

Accordingly, Pickerell's motion to dismiss all counts against him for lack of personal jurisdiction is denied.[7] Given this outcome, Openforce's request for jurisdictional discovery (Doc. 15 at 16-17) is denied as moot.

II. GigSafe's Motion To Dismiss

GigSafe moves to "dismiss all Counts of the Complaint for failure to state a claim" pursuant to Rule 12(b)(6). (Doc. 13 at 1.) GigSafe further moves to "dismiss all claims against GigSafe for lack of personal jurisdiction if the Court dismisses the breach of contract claim (Count VII)." (*Id.*) As noted, Pickerell joins in all of GigSafe's Rule

[7] The parties have extensively briefed whether the MNDA and/or Openforce's customers' contacts with Arizona support the assertion of personal jurisdiction over Pickerell. It is unnecessary to reach those arguments in light of the conclusions set forth above. Likewise, it is unnecessary to address Pickerell's objections to Openforce's response evidence. (Doc. 26 at 2-3.)

12(b)(6) dismissal arguments.

A. **Legal Standard**

Under Rule 12(b)(6), "to survive a motion to dismiss, a party must allege sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *In re Fitness Holdings Int'l, Inc.*, 714 F.3d 1141, 1144 (9th Cir. 2013) (cleaned up). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)). "[A]ll well-pleaded allegations of material fact in the complaint are accepted as true and are construed in the light most favorable to the non-moving party." *Id.* at 1144-45 (citation omitted). However, the Court need not accept legal conclusions couched as factual allegations. *Iqbal*, 556 U.S. at 678-80. Moreover, "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Id.* at 678. The court also may dismiss due to "a lack of a cognizable legal theory." *Mollett v. Netflix, Inc.*, 795 F.3d 1062, 1065 (9th Cir. 2015) (citation omitted).

B. **Breach Of The MNDA (Count Seven)**

Count Seven of the complaint alleges that GigSafe breached the MNDA in three ways: (1) by soliciting Openforce's customers in violation of § 2 of the MNDA (*id.* ¶ 102); (2) by "using Openforce's Trade Secrets and Confidential Information (as that term is defined in [§ 1(a) of] the MNDA) in a manner not for the benefit of Openforce," in violation of § 1(b) (*id.* ¶ 103); and (3) "by failing to return Openforce's Trade Secrets and Confidential Information (as that term is defined in the MNDA) in compliance with [§ 1(d)]" (*id.* ¶ 104).

1. Governing Law

The MNDA provides: "This Agreement shall be subject to the laws of the State of Arizona, without reference to its conflicts of laws principles." (Doc. 1-1 at 3 § 5.) Under Arizona law, "[t]o state a breach of contract claim, a plaintiff must allege that (1) a contract existed, (2) it was breached, and (3) the breach resulted in damages." *Steinberger v. McVey* *ex rel. Cnty. of Maricopa*, 318 P.3d 419, 434 (Ariz. Ct. App. 2014).

2. The Parties' Arguments

GigSafe argues that "Openforce alleges three separate breaches" of the MNDA—namely, "(1) 'failing to return Openforce's Trade Secrets and Confidential Information' (Section 1(d)), (2) improperly soliciting Openforce customers (Section 2), and (3) 'using Openforce's Trade Secrets and Confidential Information . . . in a manner not for the benefit of Openforce' (Section 1(b))"—and that "[n]one of these theories is plausibly alleged." (Doc. 13 at 2.) As for § 1(d), GigSafe argues that the "obligation to 'return, destroy, or erase' information only applies (1) '[a]t the discretion and direction of the Disclosing Party,' and (2) upon 'expiration or termination of [the MNDA].'" (*Id.*) Because Openforce has not alleged that it "exercised its discretion or issued a direction to GigSafe to return, destroy, or erase information" (*id.* at 2-3), and because the complaint alleges that no party has terminated the MNDA (Doc. 1 ¶ 30), GigSafe argues that "Openforce has failed to allege the necessary conditions precedent to a breach of Section 1(d)" (Doc. 13 at 3). As for § 2, GigSafe argues that it only bars solicitation of customers "introduced" to GigSafe by Openforce, and Openforce has "failed to allege that 'customers' GigSafe purportedly solicited were introduced by Openforce." (*Id.*) GigSafe also argues that § 2 excludes customers which "the Parties have previously engaged with or been presented" and that "[t]he Complaint fails to allege that the customers do not fall within this exclusion." (*Id.*) As for § 1(b), GigSafe argues that "assuming that this breach allegation refers to use of information provided under the MNDA to access the Openforce systems," the complaint fails to identify "what exactly this information is," and "[i]n any event, none of th[e] nontechnical information" addressed in paragraphs 31 and 32 of the complaint "is the type of information that would have anything to do with how to access or 'hack' the Openforce systems." (*Id.* at 3-4.) Moreover, GigSafe argues that to the extent Openforce's claims rely on GigSafe's use of customer activation codes to access Openforce's systems, "[t]here are no allegations that Openforce disclosed information about the need for customer-specific activation codes or that such information qualifies as confidential under the

MNDA"—"[i]ndeed, the publicly available portion of Openforce's system clearly explains how independent contractors access the system, including through the use of activation codes." (*Id.* at 4.)[8] In a nutshell, GigSafe argues that the challenged conduct is the misuse of Openforce's confidential information obtained through GigSafe's hacking of Openforce's systems, not the use of confidential information that Openforce "disclose[d], or permit[ted] access to" per the MNDA. (*Id.* at 5.)[9]

In response, Openforce argues that "[w]hile the Complaint plausibly pleads . . . multiple breaches of the MNDA, the Court need only find one to be plausibly alleged to deny Defendants' motion with respect to this claim." (Doc. 16 at 6.) First, Openforce argues that the complaint "plausibly alleges that GigSafe breached MNDA section 1(b), which requires that the receiving party 'not use the Confidential Information of the Disclosing Party for any purpose other than expressly permitted by the Disclosing Party,' including by using the Confidential Information '(i) to compete directly or indirectly with the Disclosing Party' and '(ii) to develop products or services competitive with those of the Disclosing Party.'" (*Id.* at 6-7, quoting Doc. 1-1 at 2 § 1(b).) Citing paragraphs 3 and 42 of the complaint, Openforce argues that the complaint "alleges that GigSafe is a direct competitor," "that GigSafe sent a letter to prospective customers in which it held itself out as a cheaper Openforce alternative," and "that GigSafe used information obtained under MNDA like 'price strategy, operating mechanics, insurance offerings, three-legged stool

[8] GigSafe appears to ask the Court to deem Openforce's system webpages incorporated by reference into the complaint. (Doc. 13 at 4 n.1.) The webpages cited by GigSafe, however, do not appear in the complaint, so incorporation by reference would not be proper. Nevertheless, on a Rule 12(b)(6) motion, "[a] court may . . . consider certain materials," including "matters of judicial notice—without converting the motion to dismiss into a motion for summary judgment." *United States v. Ritchie*, 342 F.3d 903, 908 (9th Cir. 2003). Under Federal Rule of Evidence 201(b), "[t]he court may judicially notice a fact that is not subject to reasonable dispute" if it "can be accurately and readily determined from sources whose accuracy cannot be reasonably questioned." Accordingly, the Court will take judicial notice of the two Openforce webpages cited by GigSafe. (Doc. 13 at 4 n.1.)

[9] GigSafe also argues that "the MNDA does not use the language 'in a manner not for the benefit of' either party in describing prohibited uses of Confidential Information." (Doc. 13 at 3.) The Court is just as "puzzl[ed]" as Openforce regarding this argument and agrees with Openforce that the complaint doesn't allege that the MNDA uses those exact words. (Doc. 16 at 7.) This quibble does not affect the Court's analysis, as the complaint attaches—and the Court has reviewed—the MNDA in full.

strategy, strategies to mitigate labor classification risks when retaining independent contractors, and revenue models.'" (*Id.* at 7.) Openforce argues that GigSafe's motion improperly "conflat[es] [GigSafe's] misuse of information provided under the MNDA with its other—related but distinct—course of wrongful conduct in improperly accessing Openforce's systems." (*Id.*) Second, Openforce argues that the complaint plausibly alleges a breach of § 2, prohibiting the solicitation of customers. (*Id.*) Openforce urges the Court not to adopt "GigSafe's narrow reading of the term 'introduced' at this stage" of the proceedings. (*Id.* at 8.) And Openforce emphasizes paragraph 102 of the complaint, which states: "GigSafe breached the MNDA's provision barring 'any direct or indirect contact or solicitation of any customers . . . introduced to one Party by the other Party' . . . [, and] GigSafe has engaged in many affirmative solicitations of *such* customers." (Doc. 1 ¶ 102, emphasis added.)

In reply, GigSafe argues that "Openforce's theories have shifted dramatically." (Doc. 25 at 1.) GigSafe contends that because Openforce now "concedes that receipt of . . . non-technical information under the MNDA is untethered to the alleged 'hacking' described in the Complaint," and because "the Complaint does not identify a separate misuse of information received under the MNDA," "[t]he Complaint . . . fails to link 'information [GigSafe] learned during its October 2023 meeting' (i.e., information qualifying as 'Confidential Information' under the MNDA) with any actual 'misuse' under that Agreement." (*Id.*) As for § 1(d), GigSafe argues that "Openforce tacitly concedes" that the alleged breach "is not adequately pleaded . . . because Openforce fails to address this theory of breach in its Response." (*Id.* at 2-3.) As for § 1(b), GigSafe argues that "Openforce has now confirmed there were two separate courses of conduct: (1) learning information in October 2023 (pursuant to the MNDA); and (2) learning information from alleged hacking (not pursuant to the MNDA)." (*Id.* at 3.) From that premise, GigSafe argues that there is an "absence of any allegations concerning the October 2023 information actually being used for an improper purpose (e.g., to compete) as the Complaint's *only* allegation of 'use' was in relation to the hacking." (*Id.*) As for § 2, GigSafe emphasizes that "[n]owhere in the Complaint does Openforce allege that the customers solicited were *not* parties that GigSafe had previously solicited, engaged with or been presented prior to entering into the MNDA," such that GigSafe's solicitation of customers would fall under § 2's exclusionary language. (*Id.* at 4.) GigSafe reiterates its argument that none of the customers it allegedly solicited were "introduced" by Openforce. (*Id.* at 5.)

3. Analysis

As explained below, Openforce has plausibly alleged breaches of §§ 1(b) and 2 of the MNDA.[10]

a. **Section 1(b)**

Section 1(b) of the MNDA provides that "the Receiving Party" (here, GigSafe) "shall not use the Confidential Information of the Disclosing Party" (here, Openforce) "for any purpose other than expressly permitted by the Disclosing Party" and identifies various examples of prohibited uses, including "(i) to compete directly or indirectly with the Disclosing Party; [or] (ii) to develop products or services competitive with those of the Disclosing Party." (Doc. 1-1 at 2.) Section 1(a) broadly defines "Confidential Information" as "certain non-public information, including, but not limited to, information regarding: systems . . . trade secrets . . . processes . . . information regarding . . . developments . . . customer lists . . . product plans . . . sales . . . marketing plans . . . business models, methodologies, customer lists and financial information." (*Id.*)

In paragraph 3 of the complaint, Openforce alleges that "[a]t an in-person meeting in Arizona between both sides' leadership, including [Pickerell], in October 2023, Openforce shared information about its business pursuant to a non-disclosure agreement [i.e., the MNDA], including its pricing strategy, operating mechanics, insurance offerings, three-legged stool strategy, strategies to mitigate labor misclassification risks when retaining independent contractors, and revenue models." (Doc. 1 ¶ 3.) It is reasonable to infer that at least some of this information alleged to have been shared at the in-person

[10] This conclusion makes it unnecessary, at least at this stage of the case, to address the validity of Openforce's theory of breach premised on § 1(d) of the MNDA.

meeting qualifies as "Confidential Information" under § 1(a) of the MNDA, particularly because paragraph 3 of the complaint alleges that all of this information was shared "*pursuant to*" the MNDA. (*Id.*, emphasis added.) Several other paragraphs of the complaint further raise a plausible inference that "Confidential Information" (as that term is defined in the MNDA) was shared at the Scottsdale meeting. (*Id.* ¶ 12 [alleging that "trade secrets and other confidential information" was shared "pursuant to the MNDA at a meeting in Scottsdale, Arizona"]; *id.* ¶ 32 ["[A]t an in-person meeting on October 19, 2023 in Scottsdale, Arizona . . . pursuant to the MNDA, Openforce shared detailed and confidential business plans, growth strategies, insurance information, and its revenue models."].)

The critical question is whether the complaint alleges that the Confidential Information obtained at that meeting pursuant to the MNDA was actually used by GigSafe in violation of the MNDA. If the analysis were limited to paragraph 36 of the complaint, the answer would likely be no. In paragraph 36, Openforce alleges that "Pickerell . . . now armed with information learned from Openforce under the MNDA," "knew how to get [GigSafe's] employees 'inside' Openforce's systems by posing as independent contractors and procuring customer-specific access codes." (Doc. 1 ¶ 36.) As GigSafe notes, even if the need for an activation code was shared with GigSafe by Openforce at the in-person meeting, the use of those activation codes is publicly available information such that it would not qualify as "Confidential Information" under § 1(a) of the MNDA, which requires that the information be "non-public."

But Openforce does not rely solely on paragraph 36 for its breach claim. In paragraph 42, Openforce details a letter allegedly sent by GigSafe to one of Openforce's prospective customers urging the customer to consider GigSafe's services over Openforce's because Openforce would "cost[] [the customer] a king's ransom to pay and insure [its] drivers." (Doc. 1 ¶ 42.) True, one reading of this paragraph is that GigSafe used information it obtained via hacking—not information obtained at the in-person meeting—to send this letter. This reading appears to be supported by the preceding paragraph, which states that "GigSafe used the ill-gotten information *from their hacking* into Customer A-J's workflows in an attempt to poach them—in violation of the MNDA's customer non-solicitation provision." (*Id.* ¶ 41, emphasis added). GigSafe is correct that if the information used by GigSafe to poach Openforce's customers was *only* obtained via hacking, that information would not constitute information "disclosed or provided by" Openforce and would therefore not qualify as "Confidential Information" under the terms of § 1(a) of the MNDA. Nevertheless, another plausible reading of the letter detailed in paragraph 42 is that the information GigSafe used to poach the targeted customer (and other customers) came from *both* the in-person meeting and the hacking. The complaint alleges that information shared at the in-person meeting included "pricing strategy" and "insurance offerings," both of which are directly referenced in the letter detailed in paragraph 42 of the complaint. Because at least one plausible reading of the complaint supports a claim for breach of § 1(b), Count Seven is not subject to dismissal.

b. **Section 2**

Section 2 provides that "[t]he Parties agree to . . . refrain[] during the life of [the MNDA] plus six months from any direct or indirect contact or solicitation of any customers, employees or opportunities introduced to one party by the other Party." (Doc. 1-1 at 3.)

Although "courts have granted motions to dismiss on contract claims where it is clear from the unambiguous terms of the contract that the alleged conduct by the defendant does not constitute a breach of contract," *Mieuli v. DeBartolo*, 2001 WL 777447, *5 (N.D. Cal. 2001), "[i]f a contract is ambiguous, it presents a question of fact inappropriate for resolution on a motion to dismiss," *Hicks v. PGA Tour, Inc.*, 897 F.3d 1109, 1118 (9th Cir. 2018). Here, the MNDA is not clear as to what it means for one party to "introduce" the other party to a customer. Although one plausible reading of the term "introduce" would exclude customers that GigSafe obtained by hacking Openforce's systems, Openforce's broader definition of "introduce" is plausible, too. One accepted definition of "introduce" is "to bring to a knowledge of something" (Doc. 16 at 8, quoting Merriam-Webster's definition), and the complaint plausibly alleges that the poached customers were brought to GigSafe's knowledge by Openforce and its systems. Because the contractual language does not unambiguously support GigSafe's proffered interpretation, GigSafe is not entitled to dismissal at this stage of the proceedings. *See, e.g.*, *Res. Recovery Corp. v. Inductance Energy Corp.*, 2020 WL 6149844, *6 (D. Ariz. 2020) (denying motion to dismiss breach-of-contract claim because "the presence of [contractual] ambiguity precludes dismissal at this stage"); *Raygarr LLC v. Emps. Mut. Cas. Co.*, 2018 WL 4207998, *4 (D. Ariz. 2018) ("To the extent the underlying terms of the insurance policies at issue are ambiguous, the Court declines to reach any conclusive interpretation at this stage of the proceedings. The Court merely finds that Raygarr has stated a plausible claim for breach of contract. EMC's motion to dismiss Raygarr's breach-of-contract claim will be denied.").

GigSafe also argues that Openforce has failed to plausibly allege a breach of § 2 because "[t]he Complaint fails to allege that the customers do not fall within [§ 2's] exclusion." (Doc. 13 at 3. *See also* Doc. 25 at 4.) The non-solicitation provision of § 2 "excludes any customers or opportunities the Parties have previously engaged with or been presented and any employees responding to a publicly posted job opening so long as such employee was not solicited." (Doc. 1-1 at 3.) Openforce does not respond to this specific argument.

The Court is unconvinced that Openforce's failure to plead the inapplicability of the exclusion in § 2 warrants dismissal at this stage. "While this defense may have merit at a later stage, at the motion to dismiss stage the sole question is whether the complaint has stated a plausible claim for breach of contract. The complaint need not anticipate and plead around every possible affirmative defense." *Tresona Multimedia LLC v. Legg*, 2015 WL 470228, *15 (D. Ariz. 2015). *See also Golden State Equity Invs., Inc. v. All. Creative Grp., Inc.*, 2017 WL 1336842, *6 (S.D. Cal. 2017) ("Defendant argues that it owed no duty to convert the shares requested in the Conversion Notice . . . [because] 'the New Note clearly states that Plaintiff cannot issue a conversion notice to Defendant if the amount of shares contained in the conversion notice would put Plaintiff's ownership interest in Defendant's outstanding stock over 9.99%.' Defendant does not argue that conversion of the requested shares would have resulted in Plaintiff obtaining an ownership interest exceeding 9.99%, but rather, Defendant argues that Plaintiff must plead the conversion of the requested shares would *not* have had such a result. The Court is unconvinced that dismissal is warranted on that basis. Defendant's argument is less an argument that it did not have a duty to perform under the contract as much as it is an argument that Plaintiff must plead facts precluding the existence of any potential defenses that Defendant might raise. However, 'plaintiffs need not anticipate and attempt to plead around all potential defenses.'") (quoting *Xechem, Inc. v. Bristol-Myers Squibb Co.*, 372 F.3d 899, 901 (7th Cir. 2004)).[11]

C. **Misappropriation Of Trade Secrets (Counts One and Two)**

In Count One, Openforce alleges that it "is the owner of Trade Secrets" that it "has taken reasonable and extensive measures to keep secret"; that its "Trade Secrets derive independent economic value from not being generally known to, and not being readily ascertainable through proper means by, another person"; and that "[a]t no time did Openforce consent to GigSafe's or [Pickerell's] taking, using, retaining, or disclosing the Trade Secrets." (Doc. 1 ¶¶ 48-51.) Openforce alleges that "Pickerell and GigSafe misappropriated the Trade Secrets within the meaning of the DTSA." (*Id.* ¶ 52-53.) Openforce seeks damages and injunctive relief. (*Id.* ¶ 56.) Count Two is premised on nearly identical allegations, and seeks identical relief, under the AUTSA. (*Id.* ¶¶ 57-66.)

1. The Parties' Arguments

GigSafe argues that Counts One and Two "must be dismissed because Openforce fails to identify the trade secrets with sufficient particularity." (Doc. 13 at 5.) GigSafe argues that "[a]lthough Openforce dedicates over a page of its Complaint to listing Openforce's 'trade secrets and confidential information,' Doc. 1 ¶ 17, length is not a substitute for particularity." (Doc. 13 at 6.) Referring to paragraph 17 of the complaint,

[11] GigSafe also argues that if Count Seven is dismissed under Rule 12(b)(6), Openforce's remaining claims should be dismissed for lack of personal jurisdiction. (Doc. 13 at 16-17.) Because Count Seven is not being dismissed under Rule 12(b)(6), this argument fails.

GigSafe argues that "Openforce's laundry list of 'trade secrets and confidential information' is vague and non-exhaustive" because it uses language such as "span a wide variety," "including," "include," and "among other things." (*Id.*) GigSafe further argues that "Openforce makes no effort to explain which of the many items listed in paragraph 17 [of the complaint] constitute 'trade secrets' and which constitute merely 'confidential information.'" (*Id.*)

In response, Openforce argues that a complaint need not "set forth the exact trade secrets which defendants have allegedly misappropriated" and that the "majority rule" is "that complaints need only allege the trade secret in general terms or in general contours." (Doc. 16 at 9, citations and internal quotations omitted.) Openforce argues that the level of detail in paragraph 17 "suffices at the pleading stage." (*Id.* at 10.) Openforce further argues that "[t]he cases on which GigSafe relies are distinct" because they either rely on California's trade secret statute or were decided at the summary judgment stage. (*Id.* at 10-11.) Openforce concludes that "[t]he law is clear that trade secrets need not—and should not—be identified with particularity in the Complaint." (*Id.* at 11.)

In reply, GigSafe states that it "did not argue that Openforce must plead the equivalent of the Coca-Cola formula." (Doc. 25 at 6.) "Rather, GigSafe faulted Openforce for identifying nearly every aspect of its business as both trade-secret and confidential information through broad, non-exhaustive descriptors . . . ." (*Id.*) GigSafe argues that the authorities cited in its motion "establish[] that Openforce must distinguish trade secrets from confidential information, refrain from relying on non-exhaustive categories of information, and describe the trade secrets with sufficient detail to put GigSafe on notice of the claims against it and which trade secrets it allegedly used." (*Id.*)

2. <u>Analysis</u>

"A plaintiff seeking relief for misappropriation of trade secrets must identify the trade secrets and carry the burden of showing that they exist." *Imax Corp. v. Cinema Techs., Inc.*, 152 F.3d 1161, 1164 (9th Cir. 1998) (citation and internal quotation marks omitted). However, at the pleading stage, "a plaintiff need not spell out the details of the trade secret." *Arthur J. Gallagher & Co. v. Tarantino*, 498 F. Supp. 3d 1155, 1171 (N.D. Cal. 2020) (cleaned up). *See also Quintara Biosciences, Inc. v. Ruifeng Biztech, Inc.*, 149 F.4th 1081, 1085 (9th Cir. 2025) ("[T]he federal DTSA does not require a plaintiff to identify with particularity its alleged trade secrets from the start."). Instead, "the basic test is (1) whether something beyond general knowledge is being claimed and (2) whether there is enough specificity to put the defendant on notice of what the theft is about." *Arthur J. Gallagher & Co.*, 498 F. Supp. 3d at 1171. "[W]hether a DTSA plaintiff has identified information that is sufficiently particular to constitute a trade secret—information that is kept secret and derives value from not being generally known—is a question of fact. So whether a plaintiff has sufficiently particularized a trade secret under DTSA is usually a matter for summary judgment or trial." *Quintara Biosciences*, 149 F.4th at 1085.

Under these standards, Openforce has met its burden at the pleading stage to identify the trade secrets at issue. Paragraph 17 of the complaint defines "Trade Secrets" as follows:

> Openforce's trade secrets and confidential information span a wide variety of operations and business activity, including customer preferences and requirements for enrolling independent contractors in their systems, which manifest in customers' tailored enrollment workflows that meet their own individual needs; these trade secrets and confidential information similarly include the product that Openforce makes available to its customers, rendered in Manage and Openforce's other systems as, among other things, workflows containing the necessary steps that legitimate independent contractors take to enroll to do business with one of Openforce's customers. These trade secrets and confidential information further include: customer-specific pricing; the customer's terms of engagement; customer onboarding requirements; workflow-development records, processes, and procedures; strategies for insurance and regulatory compliance regarding the independent-contractor relationship; process checks for verifying enrollees' identifies and background information; company/contractor agreements; contractor/Openforce agreements; independent contractor decision documentation; insurance plan structures and their underlying forms; contractor payment processes and forms; and state-by-state variations regarding the above. These trade secrets and confidential information also include Openforce's best practices and strategies for working with independent contractors, manifested throughout the Manage software, which includes specific processes for regulatory compliance, onboarding, recruiting, and benefits. Openforce's trade secrets and confidential

> information also include the technological information that enable Openforce's industry-leading platforms, including functionalities, schematics, and diagrams of Openforce's software systems, including (a) Workflow Designer, as well as the resulting selection and arrangement of workflows it makes available to its customers, (b) Manage, and (c) Openforce's tailored and non-public administrative interfaces available only to clients with the necessary login credentials to access them. These trade secrets and confidential information further include the trial and error (both positive and negative) that Openforce undertook to create these trade secrets. All of these trade secret and confidential information described in this paragraph (collectively, the "Trade Secrets") are related to products or services that Openforce uses in, or intends to use in, interstate or foreign commerce . . . including Workflow Designer and Manage.

(Doc. 1 ¶ 17.) Counts One and Two then reiterate that "Trade Secrets, as defined above . . . relate in part to Openforce's software system, including Manage, Openforce's tailored and non-public administrative interfaces available only to clients with the necessary login credentials to access them, and the Workflow Designer and related offerings, which allows companies both large and small to manage and on-board new independent contractors, as well as the finished product created for any individual customer by the Workflow Designer in the form of customers' specific enrollment workflows (blueprints); associated documents that reveal Openforce's customers' preferences, on-boarding processes, business operations, and compliance strategies; and information related to Openforce's insurance plans, compliance strategies, and payroll offerings." (*Id.* ¶¶ 48, 58.)

Considering that, at the pleading stage, Openforce need only state a claim with facial plausibility, it's hard to imagine how the detailed list in paragraph 17 could be deemed deficient. At least some of the items included in Openforce's definition of "Trade Secrets" have been recognized by courts as meeting the standard for a trade secret. *See, e.g.*, *Graduation Sols. LLC v. Luya Enter. Inc.*, 2020 WL 9936697, *10 (C.D. Cal. 2020) ("Courts consistently find that customer lists and customer information like Plaintiff's Business Information can qualify as trade secrets. . . . Business Information includ[ing] the terms and pricing of sales contracts, customer sales histories and preferences, and other market and vendor information . . . [is] adequately alleged . . . [as] a trade secret."); *Wyatt*

Tech. Corp. v. Malvern Instruments Inc., 2009 WL 2365647, *21 (C.D. Cal. 2009), *aff'd*, 526 F. App'x 761 (9th Cir. 2013) (rejecting defendant's argument that "customer preferences do not constitute a trade secret" under California's Uniform Trade Secrets Act because "[t]he compilation of this data could be considered a trade secret").

The cases cited by GigSafe are either inapposite or support finding Openforce's allegations sufficient at the pleading stage. For example, in *GlobalTranz Enters. Inc. v. Shipper's Choice Glob. LLC*, 2017 WL 11609546 (D. Ariz. 2017), the court found that "the complaint contains sufficient identification of the trade secrets . . . [t]hat is enough to survive a motion to dismiss" where the "complaint allege[d] misappropriation of, among other things, customer lists, profit margins, and the 'needs, likes and dislikes of customers.'" *Id.* at *4-5. The court stated that "[t]hese items have been explicitly recognized by courts in Arizona as potentially qualifying as trade secrets." *Id.* at *4. Here, similarly, the alleged trade secrets include "customer preferences" and "customer-specific pricing." (Doc. 1 ¶ 17.) Moreover, quoting a case from the Northern District of Illinois, the *GlobalTranz* court stated that "trade secrets need [only] be plead in 'general terms' and claims 'for lack of specificity' will be dismissed only 'in the most extreme cases.'" *GlobalTranz*, 2017 WL 11609546 at *5 (quoting *Mission Measurement Corp. v. Blackbaud, Inc.*, 2016 WL 6277496, *5 (N.D. Ill. 2016)). Accordingly, *GlobalTranz* cuts against GigSafe's dismissal arguments here.

The same is true as to *Alta Devices Inc. v. LG Elecs., Inc.*, 343 F. Supp. 3d 868 (N.D. Cal. 2018). There, upon "[r]eviewing the [c]omplaint," the court "f[ound] that Alta allege[d] its trade secrets with sufficient particularity" where "Alta allege[d] the exact technology in question." *Id.* at 881. Here, similarly, Plaintiff has alleged the specific technology—Workflow Designer and Manage—that was misappropriated. (Doc. 1 ¶¶ 17, 48, 58.) The *Alta Devices* court further "agree[d] with Alta that because Alta's claims are based on the Confidential Information exchanged pursuant to the 2011 NDA, LGE can hardly claim it is unable to determine what trade secrets Alta gave LGE in 2011 and 2012." *Alta Devices*, 343 F. Supp. 3d at 881 (internal quotation and citation omitted). Here, too, at least some of the information at issue is alleged to have been covered by the MNDA. (*See, e.g.*, Doc. 1 ¶¶ 3, 12; Doc. 1-1 at 2 § 1(a) [defining "Confidential Information" under the MNDA to include "trade secrets"].) Finally, the *Alta Devices* court found that "Alta's allegations look more like the allegations in *TMX Funding, Inc. v. Impero Tech. Inc.*, where the court found sufficient plaintiffs' trade secret allegations when plaintiff alleged nine broad categories of trade secret information, including, among other things: '[i]ts software, source codes, data, formulas, and other technical information developed as proprietary and confidential products and services;' '[i]ts business methods and marketing plans, such as prospective customer and sales methods for attracting and retaining customers;' and '[i]ts product information, including but not limited to, cost, pricing, margin data and other financial information.'" *Alta Devices*, 343 F. Supp. 3d at 882 (quoting *TMX Funding, Inc. v. Impero Tech. Inc.*, 2010 WL 2509979, *3 (N.D. Cal. 2010)). Openforce's definition of "Trade Secrets" in paragraph 17 is similar to, if not more specific than, the broad categories found sufficient in *TMX Funding*.

GigSafe also cites *Nitfy Techs., Inc. v. Mango Techs., Inc.*, 2024 WL 4230486 (S.D. Cal. 2024), for the proposition that "labeling information as a trade secret or as confidential information is precisely the type of threadbare recital of the elements of a cause of action that is insufficient at the pleading stage." (Doc. 13 at 6, cleaned up.) But in *Nifty Techs.*, the court found that the plaintiff had "sufficiently identifie[d] what customer information [was] being asserted as a trade secret" and had simply "fail[ed] to allege sufficient facts for the [c]ourt to determine whether that information may be widely known in the industry such that trade secret protection is defeated." 2024 WL 4230486 at *7. Here, in contrast, GigSafe doesn't argue that the alleged Trade Secrets identified in paragraph 17 lack trade secret protection because they are widely known in the industry.

GigSafe also argues that Openforce's use of non-exhaustive language in paragraph 17 of the complaint—terms such as "span a wide variety," "including," "include," and "among other things"—warrants dismissal. (Doc. 13 at 6.) But even assuming that some of GigSafe's cited non-precedential cases support that line of attack, the Court respectfully declines to follow them. Paragraph 17 identifies a sufficiently detailed and defined universe of alleged trade secrets to state a plausible claim. At worst, the inclusion of the challenged non-exhaustive terms may create some uncertainty as to whether there are additional alleged trade secrets at issue, but such uncertainty can be resolved via the discovery process and does not provide a basis for dismissing the otherwise-actionable trade secrets claims in Counts One and Two.

GigSafe next faults the complaint for purportedly failing "to explain which of the many items listed in paragraph 17 constitute 'trade secrets' and which constitute merely 'confidential information.'" (Doc. 13 at 6.) But this argument is belied by a plain reading of the complaint. Paragraph 17 of the complaint defines "[a]ll of the[] trade secrets and confidential information described in this paragraph" as "Trade Secrets" (Doc. 1 ¶ 17), and the complaint later alleges that "Trade Secrets, as defined above" (*id.* ¶¶ 48, 58) constitute "trade secrets" under the DTSA and AUTSA (*id.* ¶¶ 52, 58). There is no confusion—all of the items listed in paragraph 17 are alleged to be "Trade Secrets."

Once again, the cases cited by GigSafe are unavailing. In *Zoom Imaging Sols., Inc. v Roe*, 2019 WL 5862594 (E.D. Cal. 2019), the plaintiff identified "Confidential Information" but "d[id] not claim . . . that all of this Confidential Information constitutes trade secrets." *Id.* at *4. "Rather, [the] plaintiff allege[d] that the trade secrets at issue are *part* of this Confidential Information." *Id.* (emphasis added). Accordingly, the court found that "[b]oth the list of Confidential Information and the language in paragraph 86 fail to distinguish between the Confidential Information and the trade secrets." *Id.* at *5. But Openforce's complaint does not define "Confidential Information" as including a subset of trade secrets, thereby making it impossible to discern which are trade secrets and which are mere confidential information.

Finally, *Paul Johnson Drywall Inc. v. Sterling Grp. LP*, 2024 WL 1285629 (D. Ariz. 2024), is distinguishable because it was decided at the summary judgment stage. Also, *Paul Johnson Drywall*, like *Zoom Imaging*, involved a plaintiff that failed to delineate which subset of "Confidential Information" was a trade secret. *Id.* at *23. As stated above, that is not the case here.

In sum, at this early stage of the proceedings, Openforce has met its burden of sufficiently pleading the identity of its trade secrets.

D. Fraudulent Misrepresentation And Inducement (Counts Five and Six)

In Count Five, Openforce asserts a claim for fraudulent misrepresentation premised on GigSafe's employees' misrepresentations "that each would serve as independent contractors for certain of Openforce's clients"—representations the employees made to hack into Openforce's systems, acquire information, and "create a product that competes with Openforce." (Doc. 1 ¶¶ 82-89.) In Count Six, Openforce asserts a claim for fraudulent inducement of the MNDA premised on Pickerell's and GigSafe's misrepresentation that GigSafe "was interested in a potential corporate transaction" and Pickerell's and GigSafe's "intentional hid[ing] [of] the existence of GigSafe from Openforce." (*Id.* ¶¶ 90-92.) The complaint alleges that Pickerell and GigSafe induced Openforce to enter into the MNDA, "which was a necessary condition for . . . Openforce to share sensitive, proprietary information with" Pickerell and GigSafe that they could use to "compet[e] against Openforce." (*Id.* ¶ 95.)

1. <u>Legal Standard</u>

Both sides agree that Counts Five and Six are subject to the heightened pleading requirements of Federal Rule of Civil Procedure 9(b). (Doc. 13 at 7-12; Doc. 16 at 11-14.) Rule 9(b) requires a plaintiff to "state with particularity the circumstances constituting fraud or mistake." Fed. R. Civ. P. 9(b). "To satisfy Rule 9(b), a pleading must identify 'the who, what, when, where, and how of the misconduct charged,' as well as what is false or misleading about the purportedly fraudulent statement, and why it is false." *United States ex rel. Cafasso v. Gen. Dynamics C4 Sys., Inc.*, 637 F.3d 1047, 1055 (9th Cir. 2011) (cleaned up). *See also Schreiber Distrib. Co. v. Serv-Well Furniture Co.*, 806 F.2d 1393, 1401 (9th Cir. 1986) ("We have interpreted Rule 9(b) to mean that the pleader must state the time, place, and specific content of the false representations as well as the identities of the parties to the misrepresentation."). "The circumstances constituting the alleged fraud

[must] be specific enough to give defendants notice of the particular misconduct . . . so that they can defend against the charge and not just deny that they have done anything wrong." *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1106 (9th Cir. 2003) (cleaned up).

2. The Parties' Arguments

GigSafe argues that the complaint fails to plead Counts Five and Six with the particularity required by Rule 9(b). (Doc. 13 at 7.) Because, as discussed below, Count Five is preempted by the AUTSA, the Court need only address the parties' arguments regarding Count Six.

GigSafe argues that Count Six fails to allege the "what" or "the content" of any specific representation made to induce Openforce into executing the MNDA. (*Id.*) GigSafe further argues that the complaint fails to allege who made the representation, as well as who heard it. (*Id.* at 8-9.) GigSafe further argues that the complaint is "vague as to *when* misrepresentations were made" and that "a five-month period" is insufficient to satisfy the "when" requirement under Rule 9(b). (*Id.* at 9.) Next, GigSafe argues that "Openforce makes no attempt whatsoever to allege *where* or *how* the statements were made." (*Id.*) Next, GigSafe argues that "Openforce has not plausibly pleaded that, to the extent someone made a statement representing GigSafe's interest in a corporate transaction, that representation was false when made." (*Id.*) Finally, GigSafe argues in a footnote that "[a]ny attempt by Openforce to salvage Count VI by reframing it as a fraud by nondisclosure theory should be rejected because Openforce has not pleaded that GigSafe owed a duty to Openforce, as required for a fraud by nondisclosure claim under Arizona law." (*Id.* at 11 n.3.)

In response, Openforce argues that Count Six "centers on Defendants' hiding its intent to compete with Openforce, which induced Openforce to enter into the MNDA and to share sensitive information with Defendants." (Doc. 16 at 13.) Openforce clarifies that "this claim involves concealment, which by definition is the absence of statements" and "[r]equiring specific example statement is therefore impossible." (*Id.*) Openforce also contends that fraudulent concealment claims under Arizona law do not require a duty to disclose. (*Id.*)

In reply, GigSafe argues that Openforce has "entirely abandoned" its fraudulent inducement claim, "changing from misrepresentation-based inducement claim to an *unpleaded* concealment claim." (Doc. 25 at 7-8.) GigSafe argues that "[i]nducement, not concealment, is the theory presented in the Complaint." (*Id.* at 8.) GigSafe also argues that "[e]ven if Openforce had pleaded a claim for fraudulent concealment . . . dismissal would still be necessary" because "Openforce has not alleged any action by Defendants that 'intentionally prevented Openforce from finding the truth'" as required by Arizona law. (*Id.*, citation omitted).

3. Analysis

Count Six fails to meet the heightened pleading requirements of Rule 9(b). Even accepting Openforce's argument that Count Six, although labeled as a fraudulent inducement claim, is really a fraudulent concealment claim, what Plaintiff appears to be arguing is that Openforce intentionally concealed its intention to compete with Openforce and the existence of GigSafe by making *misrepresentations* that it was interested in a corporate transaction with Openforce. (*See, e.g.*, Doc. 1 ¶ 92 [alleging that Pickerell and GigSafe "misrepresented to Openforce that it was interested in a potential corporate transaction"]; *id.* ¶ 93 [alleging that "[t]his misrepresentation was material"]; *id.* ¶ 94 [alleging that Pickerell and GigSafe "made this misrepresentation with knowledge of its falsity"]; *id.* ¶ 95 [alleging that Pickerell and GigSafe "made this misrepresentation about its intentions of competing against Openforce . . . with the intent of inducing Openforce to enter into the MNDA"].)

To that end, *Silving v. Wells Fargo Bank, NA*, 800 F. Supp. 2d 1055 (D. Ariz. 2011), is instructive. In *Silving*, "[a]lthough" the plaintiffs' claim was "captioned 'Fraudulent Concealment,'" it "allege[d] that Defendants both 'misrepresented and concealed.'" *Id.* at 1073. The court concluded this claim was subject to dismissal for two reasons. *Id.* at 1073-74. First, because the claim alleged both misrepresentation and concealment, and because Rule 9(b) requires that "a claim of false representation . . . be pled with particularity," the claim failed because it "d[id] not state the time and place of the alleged misrepresentations, and the specific content is not present for all alleged statements." *Id.* Second, turning to "the allegations of 'concealment,'" the court held that although the complaint "assert[ed] that 'Defendants prevented Plaintiffs from learning any of these truths,'" it "fail[ed] to allege with particularity . . . how Defendants went about 'preventing' Plaintiffs." *Id.* at 1074. At any rate, to the extent those allegations of concealment and prevention were based on affirmative misrepresentations, the court held that "[a]ffirmative false statements intended to conceal require particularity as discussed above." *Id.*

Here, as in *Silving*, Openforce's fraudulent inducement claim—which Openforce now argues is actually a fraudulent concealment claim—rests on both affirmative misrepresentations and concealment. And as in *Silving*, the "misrepresentation" portions of Count Six fail to meet the heightened pleading requirements of Rule 9(b). As for the "who" requirement, it is unclear whether Openforce is relying on representations made only by Pickerell (and therefore by GigSafe by virtue of Pickerell's position at the company) or is also relying on representations made by other unnamed GigSafe employees. The complaint also fails to allege to whom the representations were made. *See, e.g., World Health & Educ. Found. v. Carolina Cas. Ins. Co.*, 612 F. Supp. 2d 1089, 1096-97 (N.D. Cal. 2009) ("[P]laintiff has not pled these claims with sufficient particularity. The complaint does not identify who at CCIF made the alleged misrepresentations . . . or to whom at WHEF the misrepresentations were made.").

As for the "what" requirement, the complaint fails to allege the content of any misrepresentations, and instead generally alleges that "Pickerell and Para misrepresented to Openforce that it was interested in a potential corporate transaction." (Doc. 1 ¶ 92. *See also id.* ¶ 3 ["Para and [Pickerell] feigned interest in a potential corporate transaction with Openforce in 2023."].) These allegations fail to state what was said by Pickerell and/or GigSafe.

As for the "when" requirement, the complaint vaguely alleges that GigSafe and Pickerell "feigned interest in a potential corporate transaction with Openforce *in 2023*."

(*Id.* ¶ 3, emphasis added.) The earliest alleged contact between the parties occurred in April 2023. (*Id.* ¶ 26.) The MNDA was executed in September 2023. (Doc. 1-1 at 3.) As GigSafe correctly observes, "Openforce cannot require GigSafe to guess when, in a five-month period, GigSafe purportedly made a wrongful statement." (Doc. 13 at 9.) *See also Southland Secs. Corp. v. INSpire Ins. Sols., Inc.*, 365 F.3d 353, 372 (5th Cir. 2004) ("Several courts have held that simply outlining a four-month window during which all of the misrepresentations occurred does not satisfy the pleading standard of Rule 9(b).") (cleaned up); *President Container Grp. II, LLC v. Systec Corp.*, 467 F. Supp. 3d 158, 165 (S.D.N.Y. 2020) ("[T]his time range of several months is insufficient to plead fraud with particularity.").

Nor does the complaint satisfy the "where" requirement. Although the complaint alleges that Pickerell and GigSafe "first got in touch with Openforce" in April 2023 "at the Express Carrier's Association conference," it doesn't allege that any misrepresentations occurred at that conference and instead alleges that the parties "stayed in touch . . . throughout that summer." (Doc. 1 ¶ 26.)

Last, the complaint fails to satisfy the "how" requirement. It's unclear, for example, whether the alleged misrepresentations were made orally, over email, or in some other format.

Openforce's purported recasting of Count Six as a concealment claim does not avoid dismissal. As in *Silving*, the complaint fails to allege how Pickerell and GigSafe "intentionally hid the existence of GigSafe from Openforce." (Doc. 1 ¶ 92.) Even assuming that a fraudulent concealment claim, unlike a nondisclosure claim, does not require a duty, a fraudulent concealment claim nonetheless requires an "action by the defendant that intentionally prevented the plaintiff from finding the truth." *Wells Fargo Bank v. Ariz. Laborers, Teamsters & Cement Masons Loc. No. 395 Pension Tr. Fund*, 38 P.3d 12, 34 (Ariz. 2002), as corrected (Apr. 9, 2002). The complaint does not contain any allegations of what "action" GigSafe took to "intentionally prevent[]" Openforce "from finding the truth." *Id.* At best, a liberal reading of the complaint implies that GigSafe concealed its true intentions and the existence of GigSafe *by making affirmative misrepresentations* that GigSafe intended to enter a corporate transaction with Openforce. But if that is Openforce's theory, its fraudulent concealment claim still fails because, as explained in *Silving*, "[a]ffirmative false statements intended to conceal require particularity." 800 F. Supp. 2d at 1074.

Accordingly, Count Six—whether based on affirmative misrepresentations, fraudulent concealment, or some combination of both—fails to satisfy Rule 9(b)'s heightened pleading requirements and is therefore dismissed.

E. AUTSA Preemption (Counts Three, Four, Five, Eight, And Nine)

GigSafe argues that Counts Three (tortious interference with contract), Four (tortious interference with business expectancy), Five (fraudulent misrepresentation), Eight (unfair competition), and Nine (unjust enrichment) are preempted by the AUTSA. (Doc. 13 at 12-14.)

1. Legal Standard

The AUTSA "creates an exclusive cause of action—and displaces conflicting causes of action—for claims based on the misappropriation of trade secrets." *Orca Commc'ns Unltd., LLC v. Noder*, 337 P.3d 545, 546 (Ariz. 2014). However, the "AUTSA does not displace common-law claims based on alleged misappropriation of confidential information that is not a trade secret." *Id.*

The AUTSA defines "Trade secret" as "information, including a formula, pattern, compilation, program, device, method, technique or process, that both: (a) Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use. (b) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy." A.R.S. § 44-401(4). A court commits error if it dismisses a "claim on preemption grounds" if that "claim, as alleged, is not limited to trade secrets." *Orca*, 337 P.3d at 548.

…

2. The Parties' Arguments

GigSafe argues that "the gravamen of Openforce's AUTSA claim is the alleged misappropriation of information through Openforce's enrollment process" and that the complaint's definition of "Trade Secrets" includes "enrollment workflows," "the product that Openforce makes available to its customers," and "Openforce's tailored and non-public administrative interfaces available only to clients with the necessary login credentials." (Doc. 13 at 13.) GigSafe argues that the same "liability and injury theory underlying" the AUTSA claim also underlies Counts Three, Four, Five, Eight, and Nine. (*Id.* at 14.) At bottom, GigSafe argues that because "the Complaint makes no effort to differentiate between which information [Openforce] alleges constitutes 'trade secrets' and which information constitutes merely 'confidential information,'" the claims are preempted by the AUTSA. (*Id.*)

In response, Openforce argues that the challenged claims are not preempted by the AUTSA because each "involves the misappropriation of trade secrets *and* confidential information." (Doc. 16 at 14.) Alternatively, Openforce contends that the challenged claims are not preempted to the extent they "involve 'conduct' that goes beyond 'misappropriation of trade secrets.'" (*Id.*)

In reply, GigSafe argues that "Openforce is trying to have their cake and eat it too." (Doc. 25 at 10.) GigSafe argues that, "[o]n the one hand, with respect to the trade-secret claim, Openforce dismisses GigSafe's argument that Openforce did not sufficiently distinguish it trade secrets from its confidential information," yet "[o]n the other hand, with respect to GigSafe's preemption argument, Openforce suggests the trade secrets and confidential information are clearly two different categories of information." (*Id.*) GigSafe also disagrees with Openforce's argument that "dismissal on preemption grounds is never appropriate because whether the information is a trade secret will depend on further discovery and litigation." (*Id.*) GigSafe concludes that Openforce "does not attempt to distinguish between confidential information underlying the tort claims and the trade secrets underlying the AUTSA claim." (*Id.* at 11.)

3. Analysis

Paragraph 17 of the complaint provides a list of "Openforce's trade secrets and confidential information" and defines "[a]ll of these trade secrets and confidential information in this paragraph" as "collectively, the 'Trade Secrets.'" (Doc. 1 ¶ 17.) In Count Two, Plaintiff asserts a claim for misappropriation under the AUTSA. (*Id.* ¶¶ 57-66.) Count Two alleges that "Openforce is the owner of Trade Secrets, as defined above" (*id.* ¶ 58)—referring to "Trade Secrets" as defined by paragraph 17. Count Two further alleges that "[t]hese Trade Secrets"—using the defined term from paragraph 17—"constitute 'trade secrets' under Arizona Rev. Stat. § 44-401(4)." (*Id.* ¶ 58.) Therefore, the complaint unambiguously alleges that the trade secrets and confidential information alleged to be "Trade Secrets," as that term is defined in paragraph 17, are also all "trade secrets" as defined by the AUTSA.

a. **Count Three (Tortious Interference With Contract)**

In Count Three, Openforce asserts a claim for tortious interference with contract. (Doc. 1 ¶¶ 67-74.) Count Three alleges that "GigSafe and [Pickerell] used the Trade Secrets and confidential information acquired by GigSafe's employees to create a product that competes with Openforce." (*Id.* ¶ 72.) Openforce argues that Count Three is not preempted because it "involves misappropriation of trade secrets *and* confidential information." (Doc. 16 at 14.) But by Openforce's own admission, at least part of this claim relates to the misappropriation of trade secrets. (*Id.*) To the extent it does, it is preempted by the AUTSA.

Of course, Count Three purports to allege the misappropriation of "Trade Secrets *and confidential information*." (Doc. 1 ¶ 72, emphasis added.) Although the "AUTSA does not displace common-law claims based on alleged misappropriation of confidential information that is not a trade secret," *Orca*, 337 P.3d at 546, the problem is that the allegations in Count Three cannot plausibly be read as covering both Trade Secrets (as defined by the complaint and as encompassed by the AUTSA) and confidential information that does not rise to the level of a statutory trade secret.

Smoketree Holding LLC v. Apke, 2023 WL 6377272 (D. Ariz. 2023), is instructive. There, the plaintiff "argue[d] that its complaint defines 'Trade Secret' to include both confidential information that rises to the statutory definition of a trade secret and confidential information that does not meet the statutory definition of a trade secret." *Id.* at *3. The plaintiff argued that several of its claims were thus not preempted by the AUTSA because they "are based on misappropriation of the confidential information that does not meet the statutory definition of a trade secret." *Id.* The court disagreed, holding that the plaintiff's "complaint, as presently drafted, is not reasonably read as covering both trade secrets and confidential information that does not rise to the level of a trade secret." *Id.* The court further noted that the nowhere "does the complaint define 'confidential information' or otherwise give Defendants fair notice of what sort of information forms the basis of the tort claims, rather than the statutory misappropriation of trade secrets claims." *Id.* Accordingly, the court held that "as presently drafted," the plaintiff's claims were "predicated on an alleged trade secret, [and] they are preempted by AUTSA." *Id.*

Here, as in *Smoketree*, Openforce's use of the defined term "Trade Secrets" in Count Three cannot plausibly be interpreted as covering both trade secrets as defined by the AUTSA and confidential information that does not meet the AUTSA's statutory definition of a trade secret, for the simple reason that the complaint defines all of the trade secrets and confidential information listed in paragraph 17 of the complaint as "Trade Secrets" and further alleges that those "Trade Secrets" all meet the AUTSA's statutory definition of trade secrets. Although Count Three uses the phrase "Trade Secrets *and confidential information*" (Doc. 1 ¶ 72, emphasis added), as in *Smoketree*, the complaint fails to define "confidential information" or "otherwise give Defendants fair notice of what sort of information forms the basis of the tort claims, rather than the statutory misappropriation of trade secrets claims." *Smoketree*, 2023 WL 6377272 at *3.

Bureau Veritas Tech. Assessments LLC v. Brosa, 2025 WL 3442766 (D. Ariz. 2025), also supports this result. There, the plaintiffs "argue[d] that their unfair competition claim is based on the misappropriation of 'confidential information,' not trade secrets." *Id.*

at *13. Although the complaint defined such confidential information to include "customer specific project management software applications," the court noted that "that category of information was successfully pled as a trade secret." *Id.* Thus, "[a]s currently pled, the unfair competition claim against Defendant Brosa is preempted under AUTSA." *Id.* Similarly, Count Three alleges that "GigSafe and [Pickerell] directed GigSafe's employees and agents to sign up or enroll on Openforce's platform as independent contractors for Customers A-J for the purposes of learning Openforce's workflows as to each of Customers A-J." (Doc. 1 ¶ 71.) But paragraph 17 of the complaint alleges that these "workflows" are "Trade Secrets." (*Id.* ¶ 17 [defining "Trade Secrets" as, *inter alia*, "customers' tailored enrollment workflows that meet their own individual needs," "workflows containing the necessary steps that legitimate independent contractors take to enroll to do business with one of Openforce's customers," and "Workflow Designer, as well as the resulting selection and arrangement of workflows it makes available to its customers"].)

Cadence Bank v. Heritage Fam. Offs. L.L.P., 2024 WL 962174 (D. Ariz. 2024), which Openforce cites, does not compel a different result. There, the court held that "whether information constitutes a trade secret is a question of fact," and "[b]ecause these claims could plausibly encompass non-trade-secret information, the claims cannot be preempted at this stage in the litigation." *Id.* at *6. But the complaint here fails to identify any confidential information that does not also qualify as "Trade Secrets" (as the complaint defines that term).

Finally, the Court is unconvinced by Openforce's contention that Count Three escapes preemption because it "involve[s] 'conduct' that goes beyond 'misappropriation of trade secrets'"—i.e., it alleges that "GigSafe targeted specific contracts and business relationships," which is "conduct going beyond misappropriation." (Doc. 16 at 14.) As pleaded, the "conduct" alleged in Counts Three is GigSafe's hacking into Openforce's systems to misappropriate Openforce's trade secrets and GigSafe's use of those trade secrets to take Openforce's business. (Doc. 1 ¶¶ 71-72.) That is the same "conduct" alleged as misappropriation in the AUTSA claim: "Pickerell and GigSafe misappropriated the Trade Secrets in the ways described above and incorporated herein, including by . . . using them in direct competition with Openforce." (*Id.* ¶ 63.) Because Count Three "appears exclusively based on misappropriation of [Openforce's] trade secret[s]," *Modulus Glob. Inc. v. Quintzy FZE LLC*, 2023 WL 6147567, *2 (D. Ariz. 2023), it is preempted.

b. **Count Four (Tortious Interference With Business Expectancy)**

Count Four does not mention "Trade Secrets" or "confidential information." (Doc. 1 ¶¶ 75-81.) Instead, it alleges that "GigSafe and [Pickerell] used the *information* acquired by GigSafe's employees." (*Id.* ¶ 79, emphasis added.) Regardless of this wordsmithing, the analysis is the same as under Count Three. At bottom, the only alleged misconduct underlying Count Four is the misappropriation of "information" that is defined elsewhere as Openforce's "Trade Secrets." Accordingly, Count Four is preempted.

c. **Count Five (Fraudulent Misrepresentation)**

Count Five alleges that Defendants (or their agents) made misrepresentations that enabled them to misappropriate "information" that they then used to unfairly compete with Openforce. (*Id.* ¶ 89 ["As a direct result of GigSafe's conduct, Openforce has suffered injury. . . . GigSafe and [Pickerell] used the information acquired by GigSafe's employees through fraud to create a product that competes with Openforce. At least three of Customers A–J have left or will leave Openforce, and two of Customers A–J are listed as customers on GigSafe's website."].) As with Count Four, this "information" is defined elsewhere as Openforce's Trade Secrets. It follows that Count Five is preempted, too.

d. **Count Eight (Unfair Competition)**

Count Eight alleges that "Openforce owns confidential information" and "maintains that this information qualifies as trade secrets as defined above and under both the DTSA and AUTSA." (Doc. 1 ¶ 110.) However, Count Eight alleges in the alternative that "to the extent that this information is determined to not qualify as a trade secret, Openforce maintains that this information qualifies as confidential, including because Openforce has taken appropriate measures to keep this information secret." (*Id.*)

In *GlobalTranz*, the court permitted the plaintiff's unfair competition claim to proceed to the extent "the claim can be read as an alternative to the trade secret claims." 2017 WL 11609546 at *7. Relying on *Orca*, the court held that "[i]f the information allegedly misappropriated does not qualify as trade secrets, it qualifies as confidential and, therefore, can support an unfair competition claim." *Id.* Although not all Arizona courts have agreed with this approach, *see Ariz. Grain Inc. v. Barkley Ag Enters. LLC*, 2020 WL 1821155 (D. Ariz. 2020), the Court finds it persuasive and thus agrees that Count Eight is not subject to dismissal at this early stage of the case. *See also* Fed. R. Civ. P. 8(d)(2) ("A party may set out 2 or more statements of a claim . . . alternatively or hypothetically, either in a single count . . . or in separate ones."). *Cf. Lacey v. Maricopa Cnty.*, 693 F.3d 896, 918 n.10 (9th Cir. 2012) (en banc) ("We note that the complaint pleads alternative facts about who ordered the arrests and how they were ordered. This is permissible.") (citation omitted).

e. **Count Nine (Unjust Enrichment)**

Count Nine is preempted because it is premised exclusively on the misappropriation of trade secrets. Count Nine alleges that "Openforce owns Trade Secrets, as defined above"; that "Pickerell and GigSafe misappropriated the Trade Secrets . . . including by acquiring, retaining, and using Openforce's trade secret information"; that "Pickerell and GigSafe used the Trade Secrets"; that "Pickerell and GigSafe have economically benefited from their use of Openforce's Trade Secrets"; that "[a]t no time did Openforce consent to GigSafe's or [Pickerell's] using the Trade Secrets"; and that "[it] would be inequitable and unjust to allow Defendants to retain the economic benefits conferred upon them by stealing Openforce's Trade Secrets." (Doc. 1 ¶¶ 117-19.) Elsewhere, the complaint clarifies that information defined as "Trade Secrets" in the complaint also "constitute[s] 'trade secrets' under" the AUTSA. (*Id.* ¶ 58.) Openforce's argument that "the unjust enrichment claim . . . could also encompass confidential information falling short of a legal trade secret" (Doc. 16 at 15) is thus without merit, as that argument is directly contradicted by the allegations in the complaint. *Smoketree*, 2023 WL 6377272 at *3-4 (dismissing unjust enrichment claim "predicated on an alleged trade secret").

F. **Economic Loss Rule**

GigSafe moves to dismiss Counts Three, Four, and Eight as barred by the economic loss rule ("ELR"). (Doc. 13 at 14-16.) However, as discussed above, Counts Three and Four have now been dismissed based on AUTSA preemption. Accordingly, it is only necessary to analyze the applicability of the ELR in relation to Count Eight.

1. Legal Standard

The ELR limits "a contracting party to contractual remedies for the recovery of economic losses unaccompanied by physical injury to persons or other property." *Flagstaff Affordable Hous. Ltd. P'ship v. Design All., Inc.*, 223 P.3d 664, 667 (Ariz. 2010). The doctrine is not applied mechanically and instead requires the court to consider the "relevant policy concerns" presented by the individual factual situation. *Id.* at 673. One such policy consideration is the different purposes that contractual and tort remedies serve: "Generally, contract law enforces the expectancy interests between contracting parties and provides redress for parties who fail to receive the benefit of their bargain. . . . Tort law, in contrast, seeks to protect the public from harm to person or property." *QC Constr. Prods., LLC v. Cohill's Bldg. Specialties, Inc.*, 423 F. Supp. 2d 1008, 1015 (D. Ariz. 2006) (quoting *Carstens v. City of Phx.*, 75 P.3d 1081, 1083 (Ariz. Ct. App. 2003)).

2. The Parties' Arguments

GigSafe argues that "if the Court finds that the Complaint sufficiently alleges a breach of the MNDA in the form of either improper solicitation of customers under the MNDA or improper use of Openforce's purported 'Trade Secrets,' then the [ELR] bars Openforce's tortious interference and unfair competition claims." (Doc. 13 at 15.) Relying on *BMO Harris Bank NA v. Corley*, 2022 WL 4781944 (D. Ariz. 2022), GigSafe argues that where "the conduct giving rise" to a tortious interference claim "is the exact same conduct giving rise to" the breach of contract claim—"i.e., the improper solicitation of clients while using confidential information"—the ELR will bar the tortious interference claim. (*Id.*, cleaned up.) GigSafe argues that because "[t]he alleged conduct giving rise to

Openforce's breach of contract claim is no different from that described in Counts III, IV, and VIII," those claims are barred by the ELR. (*Id.* at 16.)

In response, Openforce argues that "[t]he harms arising out of Openforce's tortious interference and unfair competition claims go far beyond the 'subject of' the MNDA between Openforce and GigSafe." (Doc. 16 at 15.) Openforce argues that although the complaint alleges that GigSafe violated the MNDA by "misusing information it learned under" the MNDA, "this misconduct is *not* the sole subject of Openforce's tortious interference or unfair competition claims" because those claims also allege that GigSafe hacked into Openforce's systems and used that information to compete with Openforce. (*Id.* at 15-16.) Openforce argues that the hacking "allegations do not implicate the MNDA, so the alleged harm for these claims is not" the subject of the MNDA. (*Id.* at 16.)

In reply, GigSafe reiterates that it "made clear that the [ELR] applies *only if* the Court determines that Openforce adequately pleaded a breach of the MNDA claim." (Doc. 25 at 11.)

3. Analysis

To the extent Count Eight is premised on the misappropriation of confidential information improperly accessed at the in-person meeting pursuant to the MNDA, it may be barred by the ELR. However, to the extent that Count Eight is premised on the misappropriation of confidential information acquired via GigSafe's hacking of Openforce's systems, it is not barred by the ELR. The MNDA defines "Confidential Information" as including "Trade Secrets" which the "Disclosing Party" "disclose[s], or permit[s] access to." (Doc. 1-1 at 2 § 1(a).) Confidential information obtained when GigSafe's employees hacked Openforce's systems would not have been "disclosed" by Openforce and Openforce did not "permit access" to that information under the terms of the MNDA.

Because Count Eight is not entirely subject to dismissal based on the ELR, Defendants' request to dismiss Count Eight at this early stage of the case is denied. *Rich v. BAC Home Loans Servicing, LP*, 2013 WL 10104610, *8 (D. Ariz. 2013) ("The Court finds it unnecessary to parse out Plaintiffs' various allegations and rule that some theories are adequate while others are not. On a Rule 12(b)(6) motion, Defendants may move to dismiss 'a claim,' not to dismiss or strike specific allegations or portions of a claim.").[12]

III. Leave to Amend

Consistent with Rule 15(a)(2)'s textual mandate to "freely give leave" to amend and the Ninth Circuit's exhortation to apply this mandate with "extreme liberality," *Owens v. Kaiser Found. Health Plan, Inc.*, 244 F.3d 708, 712 (9th Cir. 2001) (citation omitted), the Court will give Openforce an attempt to amend the counts being dismissed in this order.

Accordingly,

IT IS ORDERED that:

1. Pickerell's motion to dismiss (Doc. 12) is **granted in part and denied in part**. To the extent Pickerell's motion is brought pursuant to Rule 12(b)(2), the motion is denied. To the extent Pickerell's motion is brought pursuant to Rule 12(b)(6), it is granted in part and denied in part consistent with the Court's ruling on GigSafe's motion to dismiss.

2. GigSafe's motion to dismiss (Doc. 13) is **granted in part and denied in part**.

3. Openforce may file a First Amended Complaint ("FAC") within 14 days of the issuance of this order. Any changes shall be limited to attempting to rectify the deficiencies identified in this order. Openforce shall, consistent with LRCiv 15.1, attach a redlined version of the pleading as an exhibit.

Dated this 30th day of January, 2026.

Dominic W. Lanza
United States District Judge

[12] This conclusion also makes it unnecessary to address whether Count Eight, to the extent it is premised on the solicitation of customers, is barred by the ELR.