

**UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

APPLIED SYSTEMS, INC.,

Plaintiff,

v.

PBC CONSULTING INC., and ARDENT
LABS, INC., d/b/a COMULATE,

Defendants.

No. 25 CV 14251

Judge Manish S. Shah

MEMORANDUM OPINION AND ORDER

Plaintiff Applied Systems, Inc. sells insurance agency management software called Epic. Defendant Ardent Labs, Inc., d/b/a Comulate, developed software that integrates with the Epic software. To gain access to Epic and its software development kit to develop its product, Comulate created a fake company, PBC Consulting, that it held out as an insurance agency. PBC and Applied entered into agreements for PBC's use of the Epic software and its software development kit. Applied discovered anomalous use of its software, and tracked the use to PBC and eventually, Comulate. Applied sued PBC and Comulate for misappropriation of trade secrets, breach of contract, breach of the covenant of good faith and fair dealing, fraudulent misrepresentation, fraudulent inducement, conspiracy, violations of the Computer Fraud and Abuse Act, and unjust enrichment. Defendants move to dismiss the complaint. For the reasons discussed below, the motion is granted in part and denied in part.

I. Legal Standards

A complaint requires only “a short and plain statement” showing that the plaintiff is entitled to relief. Fed. R. Civ. P. 8(a)(2); *Ashcroft v. Iqbal*, 556 U.S. 662, 677–78 (2009). To survive a motion to dismiss under Fed. R. Civ. P. 12(b)(6), the plaintiff must allege facts that “allow[] the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Iqbal*, 556 U.S. at 678. “Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements” are insufficient. *Id.*

At this stage, I accept all factual allegations in the complaint as true and draw all reasonable inferences in the plaintiff’s favor. *Id.*

II. Facts

Plaintiff Applied Systems is a cloud-based software developer specializing in insurance automation software for agency and brokerage management systems. [54] ¶ 23.¹ Its core product is Epic, an insurance agency management system. [54] ¶¶ 24, 31. Epic is a platform for insurance agencies or brokerages to manage sales, policies, and customer service. [54] ¶ 24. It is also an accounting software program that enables management and reconciliation of accounts receivable and payable. [54] ¶ 24. Epic’s general ledger module allows users to enter receipts, process disbursements, create journal entries, and perform reconciliations for bank accounts and direct bill commissions. [54] ¶ 24 n.3. Integrated into Epic’s general ledger is Applied Pay, an

¹ Bracketed numbers refer to entries on the district court docket. Referenced page numbers are taken from the CM/ECF header placed on the top of filings. The facts are taken from plaintiff’s amended complaint, [54].

agency-bill accounts-receivable application that automates the process of sending invoices to insureds and processing and returning their online payment transaction data to the agency management system for reconciliation. [54] ¶ 32.

Epic offers a software development kit that allows customers to integrate third-party software with Epic. [54] ¶ 33. Applied has different software licenses depending on whether the customer needs access only to Epic via the user interface or needs to facilitate integrations using the software development kit. [54] ¶¶ 34–35. Access to the software development kit is governed by license agreement tailored to the customer's needs. [54] ¶ 35. All license agreements prohibit customers from allowing third-party access to Applied's software development kit unless the third-party provides technical services to the customer and Applied and the third-party execute an agreement. [54] ¶ 36. The third-party must assume all of the confidentiality obligations assumed by the customer and only use the software development kit for the customer's benefit in the course of the customer exercising the rights it is granted under its own agreement with Applied. [54] ¶ 36.

Epic can either be accessed via the web or its software development kit. [54] ¶ 37. Its web-based interface permits a user to interact with Epic in a conventional manner by clicking on buttons, selecting items from menus, entering data into forms, and other similar actions. [54] ¶ 37. The software development kit-based interface permits customer software to issue programmatic requests to Epic through the software development kit. [54] ¶ 37. Users of the software development kit can access some, but not all, of Epic's functions. [54] ¶ 37.

Applied says the “unique and confidential methods, processes, logic and algorithms underlying Epic’s software development kit methods” and other actions that can be initiated in Epic’s web-based user interface constitute trade secrets. [54] ¶ 38. Applied alleges ten separate algorithms that it says are trade secrets. [54] ¶¶ 45–54. It says that there is no way to legitimately reverse engineer its trade secrets, and the only conceivable way to do so is by engaging in excessive, repetitive system testing beyond any “normal” use of Epic or its software development kit. [54] ¶¶ 41, 57.

Defendant Comulate was founded in 2022 to offer an artificial intelligence tool that automated the process of revenue reconciliation within an already established agency management system (like Epic). [54] ¶¶ 58–59. Comulate and Applied entered into a pilot agreement to explore integrating their software products. [54] ¶ 61. Under this agreement, Applied gave Comulate a six-month license to access and use certain Applied products, including a software development kit key for unlimited calls to integrate Epic with Comulate’s software, a data lake, and Applied Epic, with use limited to testing the interface and electronic exchange of information between Applied Epic and Comulate’s product. [54] ¶ 62.

Since 2022, several Applied customers also became Comulate customers and sought to integrate Comulate with Epic. [54] ¶ 64. Applied authorized about sixty

customers' integrations with Comulate software using Applied's software development kit. [54] ¶ 64.²

In January 2023, a person purporting to be Jordan Bates reached out to Applied about licensing Epic for PBC Consulting, Inc., a startup insurance agency. [54] ¶ 69. In March 2024, PBC entered into two agreements (the master agreement and the software development kit schedule) with Applied for access to Epic and its software development kit. [54] ¶ 70. The master agreement restricted PBC's use of Epic, the software development kit, and any other Applied software to use in connection with PBC's internal insurance operations or solely in connection with managing PBC's insurance agency or brokerage. [54] ¶ 74. Users were "provisioned on a Named Basis only." [54] ¶ 73.

The master agreement prohibited PBC from disassembling, decompiling, reverse-engineering, modifying, transforming, translating, or attempting to gain unauthorized access to Epic's software, including its source code. [54] ¶ 78. It also prohibited the use of Epic's software to develop a competing software product or service. [54] ¶ 78. The schedule includes similar restrictions. [54] ¶ 78. The master agreement also prohibits the creation of derivative works from Applied's software, and says if PBC violates this section, it "automatically assigns to Applied, upon creation, all right, title, and interest in and to such materials, including copyright and any other intellectual property interests." [54] ¶ 79. The schedule similarly

² Applied later found out that dozens of additional Applied customers had integrated Comulate's system to Epic using Applied's software development kit without authorization. [54] ¶ 64.

prohibits modifications or derivative works and automatically assigns title to any such works to Applied. [54] ¶ 79. PBC also agreed that it would treat Applied's confidential information "not less than is reasonable under the circumstances." [54] ¶ 81.

The software development kit schedule limited the scope of PBC's software development kit license to the authorized purpose of developing an integration between HubSpot and Applied Epic via the software development kit. [54] ¶ 75. PBC agreed that its integration with HubSpot would be part of its normal business operations. [54] ¶ 75. The schedule also limited the license to authorized integrations and for internal purposes only, and PBC was not allowed to use any knowledge it gained from access and use of the software development kit to develop, create, link, or connect other interfaces, integrations, or tools unless expressly authorized by the agreement. [54] ¶¶ 75, 77, 82.

Applied's internal systems flagged PBC's use of Epic as suspicious based on an "enormous" call volume that PBC was making to Applied endpoints despite PBC's small size. [54] ¶ 95. Applied looked into it and learned that PBC's call volume exceeded the activity levels of even some of Applied's largest enterprise clients. [54] ¶ 97. In all, PBC made millions of calls to certain software development kit methods in Epic. [54] ¶ 42. Applied also discovered that the IP addresses used by PBC were IP addresses typically associated with Comulate. [54] ¶ 96.

Applied continued to investigate and discovered that PBC had more links to Comulate. [54] ¶ 98. Many PBC user credentials included the names of Comulate

employees. [54] ¶ 99. The email address used by “Jordan Bates” was associated with the LinkedIn page of a Comulate engineer. [54] ¶ 100. Applied also found that Comulate employees had attached emails directly in PBC’s Epic account in the process of testing various aspects of agency and direct billing. [54] ¶ 102. Applied found hundreds of Comulate emails in PBC’s Epic account that show Comulate testing the Epic system using fake invoices, fake customers, and even actual Applied customers’ invoices. [54] ¶ 103.

Applied says it found other indications that PBC was just a front for Comulate. [54] ¶ 104. PBC’s website was a Go Daddy shell website, PBC had no license or regulatory approval to operate as a legitimate insurance agency, it was not registered with the California Secretary of State (even though it purported to be a California company), and the PBC company address appeared to be a residential apartment building in Sacramento, California. [54] ¶ 104.

Based on these findings, Applied concluded that PBC was not a real insurance agency, and that it was in fact one-and-the-same with Comulate. [54] ¶ 96.³ Applied alleges that PBC is a sham entity created by Comulate and that it is Comulate’s alter ego. [54] ¶ 20.

Applied alleges that Comulate improperly reverse-engineered and acquired its trade secrets, including Epic’s algorithms. [54] ¶¶ 44, 114. It says that Comulate disabled client-side logging when using the Epic user interface in an apparent

³ Comulate does not dispute that PBC was not a real company. It previously conceded that PBC is not a distinct entity from Comulate. [53]. *See also* n.6, below.

attempt to conceal its activities, but that evidence shows that Comulate engaged in automated and manual crawling and scraping of the Epic user interface, particularly its agency-billing function. [54] ¶¶ 43, 92. Normal customers, Applied says, make a “modest” number of software development kit calls and actions in the Epic user interface in the performance of their day-to-day business. [54] ¶ 57. This could not be used for reverse-engineering because normal usage would not uncover the underlying methods, logic, processes, and algorithms that correspond to each individual software development kit method and certain actions accessible only through Epic’s user interface. [54] ¶ 57. But Comulate made more than twenty-five million calls during the time that it had access to Epic, which, Applied alleges, was to reverse-engineer the Epic algorithms. [54] ¶¶ 89–91.

Applied alleges that Comulate used Applied’s trade secrets to refine Comulate’s own direct-billing product to more effectively compete with Applied and ultimately sought to use Applied’s trade secrets to offer a product to replace Applied’s Epic altogether. [54] ¶¶ 43, 91, 94, 116. Applied says that Comulate needed to use the PBC account because its authorized arrangement with other Applied customers would not permit the same level of access to Epic and its software development kit. [54] ¶¶ 68, 92.

III. Analysis

A. Trade Secret Misappropriation

Comulate seeks to dismiss Applied’s trade secret misappropriation claim, arguing that the allegations are impermissibly vague and that Comulate did not misappropriate any purported trade secrets. “To prevail on a DTSA misappropriation

claim, a plaintiff must show that (1) their information was a trade secret; (2) it was misappropriated; and (3) it was used in the defendant's business." *NEXT Payment Sols., Inc. v. CLEAResult Consulting, Inc.*, 163 F.4th 1091, 1096 (7th Cir. 2026). Allegedly misappropriated information constitutes a trade secret if the owner "has taken reasonable measures to keep such information secret" and "the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information."⁴ 18 U.S.C. § 1839(3).

1. *Vague allegations*

Comulate argues that Applied's trade secrets claims are impermissibly vague because Applied did not plead specifics about the nature of the confidential data for which it claims trade secret protection. [69] at 16. I disagree.

"[Whether information qualifies as a trade secret is a question of fact that 'requires an ad hoc evaluation of all the surrounding circumstances'" and is best resolved by a factfinder. *Life Spine, Inc. v. Aegis Spine, Inc.*, 8 F.4th 531, 540 (7th Cir. 2021) (quoting *Learning Curve Toys, Inc. v. PlayWood Toys, Inc.*, 342 F.3d 714, 723 (7th Cir. 2003)); *Learning Curve Toys*, 342 F.3d at 723. To survive a motion to dismiss, "plaintiffs must only plead the existence of trade secrets in broad strokes." *Packaging Corp. of Am., Inc. v. Croner*, 419 F.Supp.3d 1059, 1065–66 (N.D. Ill. 2020); *see also*

⁴ Comulate does not dispute the independent economic value of Applied's alleged trade secrets.

Covenant Aviation Sec., LLC v. Berry, 15 F.Supp.3d 813, 818 (N.D. Ill. 2014) (“[C]ourts have found allegations to be adequate in instances where the information and the efforts to maintain its confidentiality are described in general terms.”) (collecting cases).

Applied alleges ten different algorithms that it claims are trade secrets. [54] ¶¶ 45–54. It explains what each algorithm does and how it is initiated. [54] ¶ 45 (“general ledger” algorithm performed tasks like generating and updating receivable and payable entries in the general ledger and reconciled payments and collections); ¶ 46 (“SDK-Initiated reconciliation” algorithm dealt with performing reconciliation in the general ledger); ¶ 47 (“broker” algorithm determined a list of brokers that met specific requirements, got default broker commissions, and retrieved lists of broker payable contracts that met specified parameters); ¶ 48 (“employee” algorithm retrieved a list of employees and employee commissions that met specified parameters); ¶ 49 (“attachment” algorithm retrieved a list of attachments that met specified parameters, inserted the specified attachment, and got, uploaded, and updated attachment details in Epic); ¶ 50 (“transaction” algorithm retrieved lists of transactions from Epic that met specified parameters, inserted the transactions in Epic, received transaction codes, and adjusted the commission on transactions to complete commission processes); ¶ 51 (“company” algorithm retrieved lists of companies that met the specified parameters and inserted the company payable contract in Epic); ¶ 52 (“month-end closing” algorithm generated journal entries from aggregated transactions in Epic); ¶ 53 (“UI-initiated reconciliation” algorithm

generated new general ledger entries and other data fields, reconciled transactions for user review, and updated entries on the general ledger and other data within Epic); and ¶ 54 (“invoice generation” algorithm identified billing, contact, policy, and other information from within Epic to generate an invoice based on user configurations). Applied also alleges that its algorithms are not readily ascertainable from publicly available information and describes the measures that Applied takes to keep them confidential. [54] ¶¶ 55–56, 106–13, 128. Applied requires all of its employees to sign a confidentiality, restrictive covenant, and work product agreement as a condition of employment. [54] ¶ 106. Its handbook also prohibits the improper disclosure of information, including its computer code, architecture, processes, and trade secrets. [54] ¶¶ 107–08. Applied also retains physical and electronic security at all of its offices and in all of its electronic systems. [54] ¶ 109. Customers must sign license agreements with confidentiality provisions in order to gain access to Applied’s products. [54] ¶¶ 110–13.

Applied has alleged the information (algorithms) and the efforts it has taken to maintain its confidentiality. This is sufficient to allege a trade secret.

2. *Misappropriation*

Comulate says that even if Applied has alleged that its algorithms are trade secrets, Applied has not adequately pleaded either acquisition by improper means or disclosure or use, the second element of a trade secret misappropriation claim.

Misappropriation under the Defend Trade Secrets Act means either (1) the “acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means” or (2) the “disclosure or use

of a trade secret of another without express or implied consent by a person who ... used improper means to acquire knowledge of the trade secret [or] at the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was” derived from improper means, acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret, or derived from a person who owed a duty to maintain the secrecy of the trade secret. 18 U.S.C. § 1839(5). “Improper means” includes “theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means.” 18 U.S.C. § 1839(6)(a). Reverse-engineering, by itself, is not improper means. 18 U.S.C. § 1839(6)(b).

Applied alleges that Comulate acquired its trade secrets by improper means in two ways: by reverse-engineering in breach of the contract between PBC and Applied and by using the PBC account, which gave it access it did not have with other accounts.

That the PBC account gained access to the Epic software does not mean that it acquired trade secrets by doing so. It is too big a leap to say that unauthorized access to the software necessarily implies that Comulate acquired Applied’s trade secrets. To the extent that Applied alleges trade secret misappropriation based on PBC’s access to Epic, it insufficiently alleges trade secret misappropriation.

But Applied has adequately pleaded trade secret misappropriation on a theory of reverse-engineering in violation of the PBC and Applied contract. Reverse-engineering is a breach of the contract between Applied and PBC. And the only way

that Comulate could reverse-engineer the trade secret was through misrepresentation of who was seeking the information and why. What's alleged is improper, as opposed to lawful, reverse engineering.

Although Comulate argues that Applied “fails to adduce any factual allegations supporting its ‘belief’ that PBC made a large number of method calls as a means of reverse engineering,” Applied does not need to do so. Taking inferences in Applied's favor, Comulate made an usually large number of calls—millions of them—and disabled client-side logging to conceal the fact it was doing so. [54] ¶¶ 42–43. Applied says this is indicative of reverse-engineering. [54] ¶ 41. Taking these facts as true, it is reasonable to infer that Comulate used the calls to reverse-engineer Applied's trade secrets, which is a breach of PBC's—and therefore Comulate's—duty to maintain confidentiality. [54] ¶ 81. Comulate was only able to access the software because it fraudulently held itself out as an insurance company seeking to use Applied's Epic as part of its business. It is, at this stage, a plausible story, and so can support Applied's trade secret misappropriation claim.

Applied has also alleged that Comulate is “using the trade secret it misappropriated by pretending to be PBC to refine and develop competing products.” [54] ¶ 94. Because Applied alleged that Comulate misrepresented itself to gain access and then used the acquired trade secrets to build its own products, Applied has adequately pleaded use of trade secrets in violation of Comulate's contractual duty to protect the confidentiality of Applied's software.

That Comulate had access to Epic through joint customers' accounts does not change the fact that as alleged, Comulate acquired the *trade secrets* through fraud and breach of contract. Comulate conflates access to the Epic software with access to Applied's trade secrets. Misappropriation of trade secrets requires acquisition of the *trade secrets* by improper means—not access to the software. Comulate misrepresented the way it was using Epic and used fake invoices and fake customers to test the system to acquire Applied's algorithms. [54] ¶ 103. Even if Comulate had access to Epic through other customers' accounts, it does not mean it had lawful or proper access to Applied's trade secrets.

Comulate also argues that there is an “obvious alternative explanation” for the high number of calls: that Comulate's script called certain software development kit methods in 15-minute intervals as part of ordinary operations. [69] at 14. “A complaint is too speculative where there is an ‘obvious alternative explanation’ for the complaint's factual allegations.” *Wertymer v. Walmart, Inc.*, 142 F.4th 491, 497 (7th Cir. 2025). But Comulate's explanation is not clearly “alternative”—Comulate could both continually update its data through calls every 15 minutes *and* acquire Applied's trade secrets. Whether the volume of calls was based *only* on Comulate's script and was not a way to reverse-engineer Applied's trade secrets in violation of the contract is a factual dispute best left for a factfinder.

Comulate's motion to dismiss Applied's trade secret misappropriation claim is denied.

B. Breach of Contract

Applied alleges that PBC and Comulate violated the permitted use provision of the contracts and reverse-engineered its software, used the information gained to develop its own products, and disclosed confidential information to third parties. Comulate argues that Applied's contract claims must be dismissed because they are impermissibly conclusory, that there was no alleged third party to whom Comulate disclosed confidential information, that Comulate did not build a competitive product, and that Applied failed to adequately allege damages. Comulate also argues that a constructive trust is not a remedy for breach of contract.

1. *Conclusory allegations*

Comulate says that Applied's allegations are insufficient because they are made "on information and belief." But even under the heightened pleading standard for fraud, a plaintiff may plead on information and belief if the plaintiff explains why the facts cannot be pleaded and "provide[s] 'the grounds for his suspicions.'" *United States ex rel. Hanna v. City of Chicago*, 834 F.3d 775, 780 (7th Cir. 2016) (quoting *Pirelli Armstrong Tire Corp. Retiree Med. Benefits Tr. v. Walgreen Co.*, 631 F.3d 436, 443 (7th Cir. 2011)). Rule 8(a)(2) is less demanding than Rule 9(b)'s standard for pleading fraud; courts in this district "have 'routinely' found allegations on information and belief to be sufficient to survive a Rule 12(b)(6) motion." *Robinson v. Pfister*, No. 17 CV 1051, 2019 WL 4305527, at *7 (N.D. Ill. Sept. 11, 2019) (collecting cases); *see also* 5 Wright & Miller, Federal Practice & Procedure § 1224 (West 2019) (noting that requiring allegations of the facts on which the pleader's belief is founded "seem to be unnecessary and inconsistent with the philosophy of the federal pleading

rules, except when the stricter pleading requirements” of pleading fraud and special damages apply). Applied’s allegations on information and belief are sufficient to support its breach of contract claims.

2. *Breach of confidentiality*

Comulate argues that Applied’s claims for breach of the confidentiality provisions of the master agreement and software development kit schedule are not sufficient because PBC and Comulate are the same, and so there was no disclosure to a third party. Applied says that it has alleged that PBC disclosed confidential information “at least” to Comulate, which is enough to allege disclosure to a third party. But that single phrase does not give rise to a plausible inference that PBC disclosed any confidential information to anyone other than Comulate—which is PBC.

Applied argues that Comulate demonstrated its features using its PBC account. But demonstrating how Comulate’s product works does not necessarily mean that it disclosed any confidential information. Applied does not allege what information was disclosed in the demonstration. And besides, Applied never alleged that Comulate demonstrated its product at all. It cannot amend its pleadings in its response brief. *Hardimon v. Am. River Transp. Co., LLC*, 95 F.4th 1130, 1135 n.3 (7th Cir. 2024). Applied has failed to allege a breach of contract claim based on the confidentiality provisions of the two agreements.

3. *Competing product*

Comulate also says that Applied did not “coherently allege what competitive product Comulate built, or how it used Applied’s software to build that product.” [69]

at 28. But Comulate’s argument is more about the sufficiency of the evidence than the lack of allegations. “When a defendant moves to dismiss—especially on a question of fact ... we look in a complaint only for plausibility.” *Teva Pharma. USA, Inc. v. Eli Lilly & Co.*, 181 F.4th 756, 767 (7th Cir. 2026). The complaint must present “enough details about the subject-matter of the case to present a story that holds together.” *Id.* (quoting *Swanson v. Citibank, N.A.*, 614 F.3d 400, 404 (7th Cir. 2010)).

Applied has alleged that Comulate reverse-engineered its trade secrets and used those trade secrets to refine Comulate’s own products to compete with Applied’s, and even to come up with its own replacement for Applied Epic. [54] ¶¶ 43, 91, 94, 116. These are enough facts to present a story that holds together. Whether Applied can prove those allegations is a question for a later date. At this stage, Applied has adequately alleged a breach of contract for developing competing products.

4. *Damages*

Comulate argues that Applied failed to adequately allege damages. Applied alleged that it suffered damages in the form of costs incurred investigating Comulate’s use of the PBC sandbox account. [54] ¶ 158. “Money out of pocket is a standard understanding of actual damages in contract law.” *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 830 (7th Cir. 2018). Applied spent money to investigate unusual activity in an account, which led to its discovery of Comulate’s involvement in a fraudulent account. The costs to investigate Comulate’s actions are enough to show that Applied was harmed—Applied spent money because Comulate breached the permitted use and nondisclosure provisions of the agreements. *See Avery v. State Farm Mut. Auto. Ins. Co.*, 216 Ill.2d 100, 149 (2005) (a plaintiff “must establish an

actual loss or measurable damages resulting from the breach in order to recover.”). Applied has adequately alleged damages resulting from Comulate’s alleged breach.

5. *Constructive trust*

Comulate says that a constructive trust is not a remedy for breach of contract. That’s right. “[A] breach of contract specifically has been found to *not* warrant the imposition of a constructive trust.” *Amendola v. Bayer*, 907 F.2d 760, 763 (7th Cir. 1990) (citing *Evans v. Berko*, 408 Ill. 438 (1951); *Bachewicz v. Am. Nat’l Bank & Trust*, 126 Ill.App.3d 298, 312 (Ill.App.1984), *rev’d on other grounds*, 111 Ill.2d 444 (1986)). To the extent that Comulate seeks a constructive trust for its breach of contract claims, it is not available.

C. **Implied Covenant of Good Faith and Fair Dealing**

The implied covenant of good faith and fair dealing does not give rise to an independent cause of action under Illinois law. *Bernacchi v. First Chi. Ins. Co.*, 52 F.4th 324, 330 (7th Cir. 2022). Instead, it is used in one of two ways: (1) as a construction aid “where an instrument is susceptible of two conflicting constructions, one which imputes bad faith to one of the parties and the other does not,” *id.*, and (2) where a contract “specifically vests one of the parties with broad discretion in performing a term of the contract, the covenant of good faith and fair dealing requires that the discretion be exercised ‘reasonably and with proper motive, not arbitrarily, capriciously, or in a manner inconsistent with the reasonable expectations of the parties.’” *Fox v. Heimann*, 375 Ill.App.3d 35, 42–43 (1st Dist. 2007) (*Mid-West Energy Consultants, Inc. v. Covenant Home, Inc.*, 352 Ill.App.3d 160, 165 (1st Dis. 2004)). The covenant “cannot be used to add terms in order to reach a result more equitable to

one of the parties.” *Bernacchi*, 52 F.4th at 330 (quoting *Mid-West Energy Consultants*, 352 Ill.App.3d at 165).

The master agreement and schedule granted Comulate discretion to use Epic. *See* [54-1] at 2 (§ 2.2) (“Licensee is granted a license to use the Software and services as set forth in the agreement”), 4 (§ 10.1) (“Confidential Information will be treated in the same manner that the receiving party protects its own confidential information, but not less than is reasonable under the circumstances”); [54-2] at 4 (§ 5.4) (PBC granted an “unlimited” number of transactions). Applied alleged that Comulate abused the discretion granted to it by the master agreement and schedule and used Applied’s system in bad faith. [54] ¶ 165. Comulate, as PBC, was given an unlimited number of transactions within the software development kit, and was given the discretion to protect confidential information, at a minimum, reasonably. Applied adequately alleges that Comulate acted in bad faith by acting in a manner inconsistent with the reasonable expectations of the parties in making millions of calls using the PBC account and ultimately attempting to reverse-engineer Applied’s trade secrets. Comulate did not reasonably protect Applied’s confidential information. Applied alleges a breach of contract claim based on a breach of the implied covenant of good faith and fair dealing, and it may proceed on that theory. *See Conviser v. DePaul Univ.*, 649 F.Supp.3d 686, 709 (N.D. Ill. 2023) (though breach of implied duty of good faith and fair dealing is not an independent cause of action, breach of the duty can give rise to a breach of contract claim).

D. Fraud

In order to state a claim for fraudulent misrepresentation or fraudulent inducement, a plaintiff must allege: “(1) a false statement of material fact, (2) knowledge or belief of the falsity by the party making it, (3) intention to induce the other party to act, (4) action by the other party in reliance on the truth of the statements, and (5) damage to the other party resulting from such reliance.” *Wertmyer*, 142 F.4th at 495; *Hoseman v. Weinschneider*, 322 F.3d 468, 476 (7th Cir. 2003). The reliance on the defendant’s misrepresentation must have been justified. *Cozzi Iron & Metal, Inc. v. U.S. Off. Equip., Inc.*, 250 F.3d 570, 574 (7th Cir. 2001).⁵

Comulate says that Applied has failed to allege justifiable reliance. It says that Applied could not have justifiably relied on Comulate’s statements because there were “obvious red flags” that Applied ignored. But whether reliance was justified requires many factual determinations—a factfinder “must consider all of the facts that [Applied] knew, as well as those facts [Applied] could have learned through the exercise of ordinary prudence.” *Id.* Reliance “can be determined as a matter of law when no trier of fact could find that it was reasonable to rely on the alleged statement or when only one conclusion can be drawn,” but it is “normally a question of fact.” *Id.* At this stage, a trier of fact could find that Applied reasonably relied on Comulate’s

⁵ The parties argue over whether the standard is “justifiable” or “reasonable” reliance. The Illinois courts use the terms interchangeably. See *Süd Fam. Ltd. P’ship v. Otto Baum Co., Inc.*, 2024 IL App (4th) 220782, ¶ 53 (plaintiff did not allege a false statement upon which it “reasonably relied to its detriment”) (emphasis in original); *Pack v. Maslikiewicz*, 2019 IL App (1st) 182447, ¶ 105 (“As part of its fraud claim, a plaintiff must show that its reliance on the misrepresentation was justified. ... In other words, the reliance must be reasonable.”); *Siegel Dev., LLC v. Peak Const. LLC*, 2013 IL App (1st) 111973, ¶ 114 (same).

statement that it was PBC, a startup insurance company. Companies can and should be able to reasonably rely on another company's assertion that it is the company it says it is. Whether it was reasonable for Applied to believe that Jordan Bates was real and not a liar is a question for a factfinder.

Comulate also argues that Applied's fraud claims are just a reformulation of its contract claims and so the fraud claim should be dismissed. If a plaintiff fails "to identify any fraudulent act distinct from the alleged breach of contract" and the damages the plaintiff seeks are the same damages it seeks under its breach of contract claim, the fraud claim must be dismissed as a "reformulation of the contract claim." *Greenberger v. GEICO Gen. Ins. Co.*, 631 F.3d 392, 401 (7th Cir. 2011); *Pomaranski v. Chicago Prime Packers, Inc.*, No. 23-CV-5063, 2024 WL 3950315, at *6 (N.D. Ill. Aug. 27, 2024) (damages for fraud must be different from damages from breach of contract). But although they are related, Applied's fraud claims are distinct from its contract claims. Fraudulent inducement into the contract is different from the breach of contract here—the fraud happened *before* the contract was made, while the breach was based on what happened *after* the contract was signed. *See, e.g., Five-Star AudioVisual, Inc. v. Unique Bus. Sys. Corp.*, 769 F.Supp.3d 840, 852 (N.D. Ill. 2025) (fraud claims based on allegedly false misrepresentations defendant made before entering the contract separate from breach of contract claim focused on defendant's failure to perform). Applied alleges that Comulate made a false statement of material fact when it held itself out as PBC, that Comulate knew that that was false, that Applied relied on the truth of that statement, and that, Comulate was

damaged because it had to investigate Comulate's fraudulent actions. The fraud claim is broader than the contract claim; even if PBC had not violated the contract, it would still have been fraudulent to create a fake company to induce Applied to allow Comulate to have access to Epic.

Comulate also argues that Comulate's fraud claims are preempted by the Illinois Trade Secrets Act. The Illinois Trade Secrets Act states that it "is intended to displace conflicting tort, restitutionary, unfair competition, and other laws of this State providing civil remedies for misappropriation of a trade secret." 765 ILCS 1065/8(a). In deciding the preemption issue, I need not determine whether the alleged trade secret is in fact a trade secret; I only assess whether the common law claim is *based on* the misappropriation of an alleged trade secret. *See Composite Marine Propellers, Inc. v. Van Der Woude*, 962 F.2d 1263, 1265 (7th Cir. 1992) ("Illinois has abolished all common law theories of misuse of" confidential information, so "[u]nless defendants misappropriated a (statutory) trade secret, they did no legal wrong."); *ExactLogix, Inc. v. JobProgress, LLC*, 508 F.Supp.3d 254, 268–69 (N.D. Ill. 2020); *see also CardioNet, Inc. v. Lifewatch Corp.*, No. 07 C 6625, 2008 WL 567031 (N.D. Ill. 2008) (where defendant was alleged to have fraudulently obtained heart monitor to obtain confidential and trade secret information, alleged fraud related to acquisition of the devices not preempted, but claim of fraud based on acquisition of confidential information or trade secrets contained within the devices *was* preempted). The question is whether the fraud claims would stand even if the information was not alleged to be a trade secret. *ExactLogix*, 508 F.Supp.3d at 269.

Any fraud claim based on the acquisition of confidential information or trade secrets is preempted by the Illinois Trade Secrets Act. *See* [54] ¶ 185. But claims of fraud resting on Comulate’s access to Applied’s Epic software are not preempted, because the fraud claim would stand even if the information was not a trade secret.

E. Conspiracy

Comulate moves to dismiss Applied’s conspiracy claim because PBC is an alter ego of Comulate, and one cannot conspire with oneself. Applied agrees that if PBC and Comulate are the same, then the claim should be dismissed. Comulate has argued that it is the same as PBC. Because one cannot conspire with oneself, *see McCullough v. Suter*, 757 F.2d 142, 144 (7th Cir. 1985), Applied’s conspiracy claim is dismissed.⁶

F. Computer Fraud and Abuse Act

Comulate says that Applied fails to state a claim under the Computer Fraud and Abuse Act because it does not allege that Comulate accessed a computer without authorization or exceeded authorized access nor does it allege that any unauthorized access caused Applied damages or losses of at least \$5,000. [69] at 21.

“The CFAA, 18 U.S.C. § 1030, is primarily a criminal anti-hacking statute. However, § 1030(g) provides a civil remedy for any person who suffers damage or loss due to a violation of § 1030.” *Fidlar Techs. v. LPS Real Estate Data Sols., Inc.*, 810 F.3d 1075, 1079 (7th Cir. 2016). Applied invokes § 1030(a)(2)(C), prohibiting a person from intentionally accessing a computer without authorization or exceeding his

⁶ Because Comulate conceded that PBC was a fake company, and is the same as Comulate, it is estopped from arguing otherwise in the future.

authorized access and thereby obtaining information from a protected computer. Applies also cites § 1030(a)(4), prohibiting unauthorized access with the intent to defraud, furthering the intended fraud, and obtaining anything of value.

1. Access without authorization or exceeding access

Whether a user has access to a system is a “gates-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access certain areas within the system.” *Van Buren v. United States*, 593 U.S. 374, 390 (2021). A defendant who uses “impersonations and subterfuges to circumvent those gates” and obtain information can violate the Act. *See United States v. Cuomo*, 125 F.4th 354, 365 (2d Cir. 2025). Applied alleges that Comulate used fraud to gain access. Any access that PBC had that was authorized based on fraud is a “circumvention” of the gates, and so the gates were not up for Comulate to access Applied’s system. Applied has adequately pleaded unauthorized access.

2. Damages or losses

“Loss” is defined as “any reasonable costs to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.” 18 U.S.C. 1030(e)(11).

Comulate says that because there was no actual harm to Applied’s computer data, programs, systems, or information services, there was no loss. It relies on *Van Buren*, 593 U.S. at 391–92, which observed that the statutory definitions of “damage”

and “loss” “focus on technological harms—such as the corruption of files—of the type unauthorized users cause to computer systems and data.”

There is a split in the courts in this district on whether actual technological harm is required to state a claim for “loss” under the CFAA. *Compare ExactLogix*, 508 F.Supp.3d at 265–68 (any costs resulting from responding to a potential CFAA violation offense or conducting a damage assessment sufficient to allege loss) *with Inmar, Inc. v. Vargas*, No. 18-cv-2306, 2018 WL 6716701, at *9–10 (N.D. Ill. 2018) (“loss” must relate to the impairment or disruption of a plaintiff’s computer system); *see also CCC Info. Servs., Inc. v. Tractable, Inc.*, No. 18 CV 7246, 2023 WL 415541, at *3 (N.D. Ill. Jan. 25, 2023) (taking the “middle ground” in construing “loss” to mean costs associated with the *possibility* of some type of technological damage).

“Loss” is different than “damage” under the statute, and includes the reasonable cost to a victim incurred in responding to an offense; an offense includes unauthorized intrusions that obtain information without impairing or damaging a system. *See* 18 U.S.C. § 1030(a)(2)(C), (e)(11). So long as Applied proves an offense, it can recover the reasonable costs incurred in responding to that offense. *Van Buren*’s gloss on unauthorized access and obtaining information keeps the statute’s focus on the typical consequences of hacking. *See Van Buren*, 593 U.S. at 392 (quoting *Royal Truck & Trailer Sales & Serv., Inc. v. Kraft*, 974 F.3d 756, 760 (6th Cir. 2020)). No more in terms of impairment or harm need be alleged for “loss.”

Applied's allegations plausibly allege that it incurred costs in response to PBC's unauthorized (fraudulently obtained) access. It states a claim under the Computer Fraud and Abuse Act.

G. Declaratory Judgment

Comulate moves to dismiss Applied's claim for declaratory judgment because Applied has failed to allege a derivative work or that Comulate modified or improved Applied intellectual property. Under the Declaratory Judgment Act, a district court "may declare the rights and other legal relations of any interested party seeking such declaration." 28 U.S.C. § 2201(a). Applied seeks a declaration that it is the "rightful owner of Comulate's agency billing product and direct billing reconciliation product refinements created using information from the PBC accounts." [54] ¶ 214.

The master agreement and schedule both give Applied the right to all "derivative works, modifications of," or program improvements to any Applied intellectual property. [54] ¶¶ 211–12. Applied alleges that Comulate reverse-engineered Applied's trade secrets and then used those trade secrets to "enhance the features and functionality of Comulate's direct billing reconciliation product and accelerate the development of an agency billing product." [54] ¶ 2; *see also* [54] ¶ 9 (Comulate developed an agency billing product to compete with Applied); [54] ¶¶ 12, 43, 91–92, 117, 206 (same). Applied says that Comulate's agency billing product and direct billing reconciliation product refinements constitute derivative works, modifications of, or program improvements to Epic and the software development kit. [54] ¶ 213.

Applied's allegations that Comulate's already existing product was enhanced by Applied's trade secrets does not allege a derivative work, modification, or improvement of *Applied's* intellectual property. Instead, the use of Applied trade secrets, as alleged, was a modification or improvement to *Comulate's* intellectual property. But to the extent that Applied created an agency billing product to replace Epic, that may constitute a derivative work, modification, or improvement to Applied's intellectual property, and can state a claim.

Comulate says that Applied's declaratory judgment claim is preempted by the Copyright Act. But preemption is an affirmative defense that a complaint does not need to anticipate. *Franco v. Chobani, LLC*, __ F.4th __, 2026 WL 2150193, at *1 (7th Cir. July 27, 2026). It is too early to decide whether Applied's claims are preempted, and I decline to dismiss the declaratory judgment claim on those grounds.

H. Unjust Enrichment

Applied alleges that PBC and Comulate have been unjustly enriched through their unauthorized access to Applied's software platform and their use of information derived therefrom. [54] ¶ 216. Any claim that Comulate has been unjustly enriched by its use of information derived from unauthorized access is simply restating Applied's misappropriation of trade secrets claim and is preempted. *Composite Marine*, 962 F.2d at 1265.

Unjust enrichment based on Comulate's unauthorized access to Applied's software platform is dismissed because it is not pled in the alternative to the breach of contract. Plaintiffs are allowed to bring both breach of contract and unjust enrichment claims. *See Hernandez v. Ill. Inst. of Tech.*, 63 F.4th 661, 671 (7th Cir.

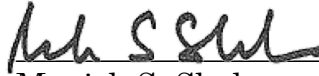
2023). But plaintiffs “may not ‘incorporate by reference allegations of the existence of a [valid] contract between the parties in the unjust enrichment count,’ because this would seek relief that Illinois does not offer.” *Id.* (quoting *Gociman v. Loyola Univ. of Chi.*, 41 F.4th 873, 887 (7th Cir. 2022)). As in *Gociman*, Applied has “inadvertently ‘incorporated by reference allegations of the existence of a contract between the parties,’” and unlike *Hernandez*, it has not expressly pleaded its unjust enrichment claim in the alternative. *Id.* at 671–72. The unjust enrichment claim is dismissed in its entirety.

IV. Conclusion

Comulate’s motion to dismiss, [64], is granted in part and denied in part. Applied’s trade secret misappropriation, breach of contract for developing competing products and for breach of the implied covenant of good faith and fair dealing, declaratory judgment, Computer Fraud and Abuse Act, and fraud claims based on access to Epic may proceed. Applied’s breach of confidentiality, unjust enrichment,

conspiracy, and fraud claims based on the acquisition of confidential information or trade secrets are dismissed without prejudice.⁷

ENTER:



Manish S. Shah
United States District Judge

Date: August 31, 2026

⁷ *Hernandez*, 63 F.4th at 671–72 (plaintiffs are “generally entitled to at least one chance to amend their complaint to cure an error in response to a district court’s dismissal order”) (internal quotation marks and citation omitted).