IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

RALLY AG LLC, Plaintiff, v. APPLE, INC., Defendant.	CIVIL ACTION NO. 1:23-cv-01106

OPINION

Slomsky, J. **November 20, 2024**

TABLE OF CONTENTS

I. INTRODUCTION 3

II. BACKGROUND 4

A. Factual Background 4

1. The '107 Patent 4

2. Defendant's "Hide-My-Email" Product 8

3. Plaintiff's Patent Infringement Allegation 9

B. Procedural Background 10

III. STANDARD OF REVIEW 10

IV. ANALYSIS 14

A. The '107 Patent Is Eligible for Protection Under § 101 14

1. Alice Step One: The '107 Patent Is Directed to an Abstract Idea 15

2. Alice Step Two: Claim 13 of the '107 Patent Provides an Inventive Concept 17

IPR2024-01446
Apple, Inc. v. Rally AG LLC
Ex. 2002

B. Plaintiff's Second Amended Complaint Plausibly Alleges a Patent Infringement Claim Against Defendant 20

V. CONCLUSION 23

I. INTRODUCTION

This case arises out of Defendant Apple, Inc.'s ("Defendant") alleged infringement of U.S. Patent No. 11,361,107 ("the '107 Patent") owned by Plaintiff Rally AG LLC ("Plaintiff"). (See Doc. No. 35 [hereinafter "SAC"].) In its Second Amended Complaint ("SAC"), Plaintiff alleges Defendant's "Hide-My-Email" product infringes on the email cloaking system covered by the '107 Patent.[1] (See id.) An email cloaking system, as described in the '107 Patent, is a system that allows parties to communicate anonymously through email. (See id.) In response to the SAC, Defendant filed a Motion to Dismiss Plaintiff's Second Amended Complaint (the "Motion"), arguing the SAC should be dismissed because the '107 Patent covers ineligible subject matter under 35 U.S.C. § 101.[2] (See Doc. Nos. 41, 42.) In the Motion, Defendant also moves under Federal Rule of Civil Procedure 12(b)(6) to dismiss Plaintiff's patent infringement claim for failure to state a claim upon which relief can be granted. (See Doc. No. 41.) For reasons that follow, Defendant's Motion to Dismiss Plaintiff's Second Amended Complaint (Doc. No. 41) will be denied.

---

[1] Plaintiff's Second Amended Complaint is the operative complaint in this case. (See Doc. No. 35.)

[2] 35 U.S.C. § 101 provides:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Patent ineligible subject matter under 35 U.S.C. § 101 are those concerning laws of nature, natural phenomena, and abstract ideas. See Alice Corp. Pty. v. CLS Bank Int'l, 573 U.S. 208, 216 (2014) ("We have long held that [Section 101] contains an important implicit exception: Laws of nature, natural phenomena, and abstract ideas are not patentable.")

II. BACKGROUND

A. Factual Background

1. The '107 Patent

Plaintiff is the owner of the '107 Patent, titled "Privacy Friendly Communication by Operation of Cloaked/Decloaked Email," which was issued by the United States Patent and Trademark Office on June 14, 2022. (SAC at ¶¶ 47-48.) The '107 Patent was originally assigned to autoGraph Inc. ("Autograph") by its inventor, Brian Roundtree.[3] (Id. at ¶¶ 40, 48.) Autograph was founded by Mr. Roundtree in early 2010 to "solve privacy issues around advertising while improving advertising performance." (Id. at ¶ 40.) To solve these issues, Autograph "developed a series of products (and obtained related patents) around the general problem of user-controlled access to personal data and [personally identifiable information] without losing control of the data itself." (Id. at ¶ 42.) In other words, Autograph's products focused on giving users a way to allow third parties to use their personally identifiable information without giving these third parties direct access to such information. (Id.) In connection with these products, Autograph developed an "email cloaking technology," which is the subject of the '107 Patent. (Id. at ¶¶ 45, 50.)

The '107 Patent is aimed at protecting the privacy of individuals communicating with third parties on the Internet. (Id. at ¶ 51.) In simple terms, the '107 Patent describes an "ID cloaking system" that allows two parties communicating through email to do so without revealing their identities. The ID cloaking system accomplishes this process by assigning each party an anonymous email address, intercepting each email sent between the parties, and replacing the "To" and "From" fields in the emails with each party's anonymous email address before forwarding the

[3] Autograph transferred ownership of the '107 Patent to Plaintiff, who "is the current owner of all rights, titles, and interests in and to the '107 Patent." (SAC at ¶ 48.)

email to the appropriate party. By assigning the parties anonymous email addresses, the '107 Patent aspires to solve the issue of data breaches, which is a common problem that plagues traditional email communications, specifically between consumers and merchants. (See id. at ¶ 34.) As the SAC notes, "it is rarely an option for a consumer . . . not to give out her personal information such as email information . . . and still conduct most any transaction in today's information centric economy." (Id. at ¶ 35.) But by giving out their email addresses, these consumers put their private emails at risk of mass exposure through data breaches. And because "[m]odern consumers frequently have become the victims of data breaches," most consumers today are bombarded with "a steady stream of emails infected with malicious code (mass-mailing worms and viruses), unwanted product advertisements (spam), and requests for personal information from criminals masquerading as legitimate entities to enable the commission of fraudulent activity (phishing)." (Id. at ¶¶ 33-34.)

More specifically, the '107 Patent's ID cloaking system operates as follows. The '107 Patent refers to the party initiating the anonymous email communications, typically the consumer, as the "end user," and the party receiving the anonymous email communications, typically the merchant, as the "relying party." (See id., Exhibit A [hereinafter "'107 Patent"].) As described in the SAC, an end user wishing to anonymously communicate with third parties, such as merchants as the relying party, can download a "web plugin browser extension" or "mobile device application" that is "configured to interact with the ID cloaking systems." ('107 Patent at 7:51-55.) With the downloading of the browser extension or mobile app, the '107 Patent's specification assumes that the end user will create "a profile/person with the identity cloaking system," at which time the end user can specify which information they want to keep private from third parties, such as their email address. (See id. at 7:58-67.) If the end user chooses to keep their email address

private, the ID cloaking system will create a cloaked email address for that end user. (See id.) The ID cloaking system stores this information in the end user's profile/persona. (See id. at 8:10-11.)

If the end user decides they do not want to share their personal email with a relying party, the browser extension or mobile app will instead give the end user the option to use their cloaked email address. (See id. at 8:26-31.) For example, if an end user fills out a form on a merchant's website and the form requires the end user to input their email address, the ID cloaking system, acting through the browser extension or mobile app, will give the end user the option to fill in the form's email address field with the end user's cloaked email address. Therefore, if the merchant chooses to email the end user in response to the completed webform, the merchant can only email the end user's cloaked email address, which the ID cloaking system will intercept.

To ensure that the ID cloaking system intercepts the email sent to the end user from the merchant/relying party, the end user's cloaked email address must end in the same domain as the domain associated with the ID cloaking system.[4] (See SAC at ¶ 56.) This is accomplished when the end user creates a profile with the ID cloaking system, at which time the ID cloaking system assigns the end user a cloaked email address that ends in the same domain as the ID cloaking system. (See '107 Patent at 7:58-67.) For example, an end user using the de-cloaked email "example@gmail.com" would be assigned by an ID cloaking system using the domain "autograph.me," a cloaked email address of "example@autograph.me." Because both the ID cloaking system and the end user's cloaked email address use the same domain "autograph.me," any email sent to this cloaked email address would first be intercepted by the ID cloaking system. Once intercepted, the ID cloaking system would "intelligently" swap the end user's cloaked email

[4] A domain is the portion of an email address that follows the "@" sign. For example, the domain in "example@gmail.com" is "gmail.com."

address for their de-cloaked email address. (SAC at ¶ 61.) To illustrate, the ID cloaking system would intercept an email sent to the end user's cloaked email address "example@autograph.me" and intelligently swap this cloaked email address for "example@gmail.com," which is the end user's de-cloaked email address. Instead of "To: example@autograph.me," the email would now read "To: example@gmail.com."

When the ID cloaking system intercepts the relying party's email to the end user, the system will also "determine whether the end user profile contains a previous association between the relying party address and a cloaked relying party address." (Id. at ¶ 56.) In other words, the ID cloaking system will search the end user's profile to determine whether the system has already assigned that particular relying party a cloaked email address. (See id.) If it has already done so, the ID cloaking system will swap the relying party's de-cloaked email address for its cloaked email address. (See id.) If the system has not already assigned the relying party a cloaked email address, the system will generate one, store the association between the relying party's cloaked and de-cloaked email addresses in the end user's profile, and then swap out the appropriate email addresses. (See id.) When generating a cloaked email address for the relying party, the ID cloaking system will assign the relying party a cloaked email address that ends in a different domain than the relying party's de-cloaked email address. (See id.) For example, a relying party using the de-cloaked email "info@nordstrom.com" would be assigned by the ID cloaking system a cloaked email address of "info@autograph.me." Once each party's respective cloaked and de-cloaked email addresses have been swapped in and out, the ID cloaking system will then forward the email to the end user's de-cloaked address, listing the relying party's "reply-to" address as its cloaked email. (See id.)

As a result, if the end user chooses to reply to the relying party's initial email, all the end user must do is click "reply" and send the email back to the relying party's cloaked email address. (Id. at ¶ 67.) The ID cloaking system will again intercept the email and swap out each party's respective cloaked and de-cloaked addresses before forwarding the email to the relying party's de-cloaked email. (See id. at ¶ 56.) Through this function, the ID cloaking system enables the parties to engage in anonymous email chain threading. (Id. at ¶ 61.)

2. Defendant's "Hide-My-Email" Product

Plaintiff alleges that Defendant's website, https://www.Apple.com/, contains a feature which is a replica of the '107 Patent's ID cloaking system. More specifically, Defendant allegedly "provides a mobile application in order to provide privacy measures to its customers and users, including but not limited to its 'Hide-My-Email' feature." (Id. at ¶ 12.) Defendant introduced its "Hide-My-Email" feature in September 2021, as part of Apple's iOS 15 platform. (Id. at ¶ 24.) "According to Defendant, the 'Hide-My-Email' product 'lets you create unique, random email addresses that forward to your personal inbox so you can send and receive email without having to share your real email address.'" (Id.)

Defendant's website provides that "[i]f you create an account with an app or visit a website that supports Sign in with Apple, you can choose to share your email address, if you're familiar with the app or visit a website, or hide your email address, if you'd prefer more privacy." (Id. at ¶ 25.) Further, "[i]f you choose the Hide My Email option, only the app or website you created the account with can use this random email address to communicate with you." (Id. at ¶ 26.) Finally, the SAC alleges that "[w]ith an iCloud+ subscription, you can generate unique, random addresses on your device with iOS 15, iPadOS 15, or macOS Monterey or later in any email field in Safari. You can also generate email addresses on-demand in the Settings app in iOS or iPadOS, in System Settings or System Preferences in macOS, in the Mail app, or on iCloud.com. [I]n iOS

16 or iPadOS 16 or later, you can also keep your email address private in third-party apps." (Id. at ¶ 27.)

3. Plaintiff's Patent Infringement Allegation

Plaintiff accuses Defendant of infringing on the '107 Patent through "all Apple devices, including iPhones and iPads, that have cloaking and decloaking capabilities." (Id. at ¶ 11.) Specifically, Plaintiff asserts that Defendant infringes on Claim 13 of the '107 Patent. (See id. at ¶¶ 78, 89.) Claim 13 provides the following:

> A non-transitory computer readable medium for a [sic] ID cloaking system having instructions stored thereon that are executable by processor electronics to: [5]
>
> > receive an email addressed to a cloaked end user address, wherein the email is sent from a relying party email address, and wherein the domain of the cloaked end user address and the domain associated to the cloaked ID system are the same domain;
> >
> > identify an end user specified address associated to the cloaked end user address by an end user profile;
> >
> > determine whether the end user profile contains a previous association between the relying party address and a cloaked relying party email address, wherein the relying party address has a different domain than the cloaked relying party email address;
> >
> > where the end user profile does not contain a previous association between the relying party address and the cloaked relying party email address, then generate a new cloaked relying party email address and associate the new cloaked relying party email address to the end user profile, the cloaked end user address, wherein the new cloaked relying party email address is generated with a domain different than the relying party address; and
> >
> > send the email to the identified end user specified address, wherein the email is configured with a reply-to email address comprising the new cloaked relying party email address.

(Id. at ¶ 56 (quoting '107 Patent at 31:8-30, 32:1-4).)

---

[5] As explained by Defendant's counsel in a hearing before the Court on March 21, 2024, a non-transitory computer readable medium "refers to something like memory or a hard disk that would store information in the computer, and non-transitory refers to the idea that it is stored in some sort of durable fashion instead of just very, very briefly, like being transmitted over the internet." (Doc. No. 32 at 12:24-25, 13:1-3.)

B. Procedural Background

On May 3, 2024, Plaintiff filed its Second Amended Complaint. (Doc. No. 35.) On May 24, 2025, Defendant filed a Motion to Dismiss Plaintiff's Second Amended Complaint and an Opening Brief in support of the Motion. (Doc. Nos. 41, 42.) On June 14, 2024, Plaintiff filed an Answering Brief in Opposition to Defendant's Motion. (Doc. No. 45.) On June 28, 2024, Defendant filed a Reply Brief in further support of its Motion. (Doc. No. 46.) On August 15, 2024, the Court held a hearing on the Motion. (See Doc. No. 49.) Defendant's Motion (Doc. No. 41) is now ripe for disposition.

III. STANDARD OF REVIEW

Under Rule 12(b)(6), a party may move to dismiss a complaint for "failure to state a claim upon which relief can be granted." Fed. R. Civ. P. 12(b)(6). To survive the motion to dismiss, the complaint need not contain "detailed factual allegations," but it must contain sufficient factual matter to "state a claim to relief that is plausible on its face." Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (quoting Bell Atl. Corp v. Twombly, 550 U.S. 544, 555, 570 (2007)). In assessing the plausibility of a claim, a court must accept all well-pleaded factual allegations in the complaint as true and draw all reasonable inferences in favor of the plaintiff. In re Rockefeller Ctr. Prop., Inc. Sec. Litig., 311 F.3d 198, 215 (3d Cir. 2002). A court's review is limited to the allegations in the complaint, exhibits attached to the complaint, and documents incorporated by reference. Mayer v. Belichick, 605 F.3d 223, 230 (3d Cir. 2010); El-Hewie v. Bergen Cty., 348 F. App'x 790, 794 (3d Cir. 2009).

It is well-settled that courts may determine patent eligibility under 35 U.S.C. § 101 at the Rule 12(b)(6) stage. SAP Am., Inc. v. InvestPic, LLC, 898 F.3d 1161, 1166 (Fed. Cir. 2018) (stating that patent eligibility "may be, and frequently has been, resolved on a Rule 12(b)(6) or (c)

motion"); FairWarning IP, LLC v. Iatric Sys., Inc., 839 F.3d 1089, 1097 (Fed. Cir. 2016) (stating that "it is possible and proper to determine patent eligibility under 35 U.S.C. § 101 on a Rule 12(b)(6) motion") (quoting Genetic Techs. Ltd. v. Merial L.L.C., 818 F.3d 1369, 1373–74 (Fed. Cir. 2016)); see also Voter Verified, Inc. v. Election Sys. & Software LLC, 887 F.3d 1376, 1379 (Fed. Cir. 2018) (affirming Rule 12(b)(6) dismissal based on § 101 patent ineligibility); Maxon, LLC v. Funai Corp., 726 F. App'x 797, 798 (Fed. Cir. 2018) (same). Determining eligibility at the pleadings stage is possible, however, "only when there are no factual allegations that, taken as true, prevent resolving the eligibility question as a matter of law." Aatrix Software, Inc. v. Green Shades Software, Inc., 882 F.3d 1121, 1125 (Fed. Cir. 2018).

As noted, Section 101 of the Patent Act provides that anyone who "invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof" may obtain a patent. See 35 U.S.C. § 101. The United States Supreme Court has recognized three exceptions to the broad categories of subject matter eligible for patenting under § 101: laws of nature, physical phenomena, and abstract ideas. Alice Corp. Pty. v. CLS Bank Int'l, 573 U.S. 208, 216 (2014). These exceptions "are 'the basic tools of scientific and technological work' that lie beyond the domain of patent protection." Ass'n for Molecular Pathology v. Myriad Genetics, Inc., 569 U.S. 576, 589 (2013) (quoting Mayo Collaborative Servs. v. Prometheus Labs., Inc., 566 U.S. 66, 77-78 (2012)); see also Alice, 573 U.S. at 216. A claim falling within any one of these exceptions is directed to ineligible subject matter under § 101. "[W]hether a claim recites patent eligible subject matter is a question of law which may contain underlying facts." Berkheimer v. HP Inc., 881 F.3d 1360, 1368 (Fed. Cir. 2018).

Courts follow a two-step "framework for distinguishing patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of those concepts." Alice, 573 U.S. at 217; see also Mayo, 566 U.S. at 77-78. First, at step one, the Court determines whether the claims are directed to one of the three patent-ineligible concepts. Alice, 573 U.S. at 217. If the claims are not directed to a patent-ineligible concept, "the claims satisfy § 101 and [the Court] need not proceed to the second step." Core Wireless Licensing S.A.R.L. v. LG Elecs., Inc., 880 F.3d 1356, 1361 (Fed. Cir. 2018). If, however, the Court finds that the claims at issue are directed to a patent-ineligible concept, the Court must then, at step two, search for an "inventive concept," – i.e. "an element or combination of elements that is 'sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself.'" Alice, 573 U.S. at 217-18 (alteration in original) (quoting Mayo, 566 U.S. at 72-73). These two steps are discussed in more detail below.

At both steps of the Alice framework, courts often find it useful "to compare the claims at issue with claims that have been considered in the now considerably large body of decisions applying § 101." TMI Sols. LLC v. Bath & Body Works Direct, Inc., No. 17-965-LPS-CJB, 2018 WL 4660370, at *5 (D. Del. Sept. 28, 2018); see also Amdocs (Israel) Ltd. v. Openet Telecom, Inc., 841 F.3d 1288, 1295 (Fed. Cir. 2016) ("[T]he decisional mechanism courts now apply [to Section 101 cases] is to examine earlier cases in which a similar or parallel descriptive nature can be seen.")

A. Step One of the Alice Framework

At step one of Alice, "the claims are considered in their entirety to ascertain whether their character as a whole is directed to excluded subject matter." Internet Patents Corp. v. Active Network, Inc., 790 F.3d 1343, 1346 (Fed. Cir. 2015); see also Affinity Labs of Texas, LLC v.

DIRECTV, LLC, 838 F.3d 1253, 1257 (Fed. Cir. 2016) [hereinafter "Affinity Labs I"] (step one looks at the "focus of the claimed advance over the prior art" to determine if the claim's "character as a whole" is to ineligible subject matter). "This 'directed to' inquiry does more than 'simply ask whether the claims involve a patent-ineligible concept'. . . Instead, we must look to the character of the claims as a whole to determine whether they are 'directed to' patent-ineligible subject matter." AI Visualize, Inc. v. Nuance Commc'ns, Inc., 97 F.4th 1371, 1378 (Fed. Cir. 2024) (citing Enfish, LLC v. Microsoft Corp., 822 F.3d 1327, 1335 (Fed. Cir. 2016)). In addressing step one of Alice, a court should be careful not to oversimplify the claims or the claimed invention because, at some level, all inventions are based upon or touch on abstract ideas, natural phenomena, or laws of nature. Alice, 573 U.S. at 217; see also McRO, Inc. v. Bandai Namco Games Am. Inc., 837 F.3d 1299, 1313 (Fed. Cir. 2016). "At step one, therefore, it is not enough to merely identify a patent-ineligible concept underlying the claim; [courts] must determine whether that patent-ineligible concept is what the claim is 'directed to.'" Rapid Litig. Mgmt. Ltd. v. CellzDirect, Inc., 827 F.3d 1042, 1050 (Fed. Cir. 2016).

B. Step Two of the Alice Framework

At step two of Alice, in searching for an inventive concept, a court looks at the claim elements and their combination to determine if they transform the ineligible concept into something "significantly more." Alice, 573 U.S. at 218; see also McRO, 837 F.3d at 1312. This second step is satisfied when the claim elements "involve more than performance of 'well-understood, routine, [and] conventional activities previously known to the industry.'" Berkheimer, 881 F.3d at 1367 (citation omitted); see also Mayo, 566 U.S. at 73. "The inventive concept inquiry requires more than recognizing that each claim element, by itself, was known in the art . . . . [A]n inventive concept can be found in the non-conventional and non-generic arrangement of known,

conventional pieces." Bascom Glob. Internet Servs., Inc. v. AT&T Mobility LLC, 827 F.3d 1341, 1350 (Fed. Cir. 2016). "A claim cannot rest on the patent-ineligible concept alone to transform the invention into something significantly more than that concept." AI Visualize, 97 F.4th at 1379 (citing BSG Tech LLC v. Buyseasons, Inc., 899 F.3d 1281, 1290 (Fed. Cir. 2018)). Fundamentally, step two "look[s] more precisely to what the claim elements add." Elec. Power Grp., LLC v. Alstom S.A., 830 F.3d 1350, 1353 (Fed. Cir. 2016).

Furthermore, whether claim elements or their combination are well-understood, routine, or conventional to a person of ordinary skill in the art is a question of fact. Berkheimer, 881 F.3d at 1368. "Thus, at the motion to dismiss stage, 'patentees who adequately allege their claims contain inventive concepts survive a § 101 eligibility analysis under Rule 12(b)(6).'" AI Visualize, 97 F.4th at 1379.

IV. ANALYSIS

In its Motion to Dismiss, Defendant argues that Plaintiff's Second Amended Complaint ("SAC") should be dismissed for three reasons: (1) the '107 Patent is directed to ineligible subject matter under § 101, specifically to an abstract idea; (2) the combined elements of Claim 13 do not transform the claim into an inventive concept; and (3) Plaintiff's SAC fails to plausibly allege a patent infringement claim against Defendant. (See Doc. No. 42 at 12, 24.) The Court will address each of these arguments in turn.

A. The '107 Patent Is Eligible for Protection Under § 101

Defendant contends that the '107 Patent is unpatentable because it fails under both steps of Alice. (Doc. No. 42 at 12, 18.) First, Defendant asserts that the claims of the '107 Patent "are directed at the abstract idea of using aliases and an intermediary as a conduit to anonymize correspondence between two people." (Id. at 6.) Stated differently, Defendant argues the '107

Patent is directed at the abstract idea of using a third party as a go-between to forward communications between two parties so that the parties can communicate without revealing their identities to one another. Second, Defendant claims that the '107 Patent contains no inventive concept. (Id. at 18.)

Plaintiff argues to the contrary, claiming the '107 Patent is eligible for patent protection under both Alice steps. (Doc. No. 45 at 11, 18.) Plaintiff first submits that the '107 Patent "is directed to an innovation that provides secure, anonymous, and end-to-end email communications between two parties that allows the email thread to remain intact through the conversation between the anonymous parties." (Id. at 6.) Next, even if the '107 Patent is directed at an abstract idea, Plaintiff contends it is nevertheless patent eligible because Claim 13 of the '107 Patent "claims an inventive concept because it recites unconventional activity that improves upon the prior art in a specific environment related only to electronic mail." (Id. at 7.)

1. Alice Step One: The '107 Patent Is Directed to an Abstract Idea

As noted above, to assess whether a claim is patent-eligible, courts engage in a two-step analysis under Alice. Regarding the first step of the Alice framework, the relevant question is whether the claims are directed to patent-ineligible subject matter. See Alice, 573 U.S. at 217. Here, the relevant inquiry is whether the claims in the '107 Patent are directed to an abstract idea.

Defendant argues that the '107 Patent is directed to "the abstract idea of using aliases and an intermediary as a conduit to anonymize correspondence between two people." (Doc. No. 42 at 6.) In support of this argument, Defendant relies on the conceptual similarity between Claim 13 of the '107 Patent and the asserted claim in Blix Inc. v. Apple, Inc., where a court held that the claim was directed to the abstract idea of "using a proxy to facilitate anonymous communications." (Doc. No. 42 at 17); Blix Inc. v. Apple, Inc., No. 19-1869, 2020 WL 7027494, at *4 (D. Del. Nov. 30, 2020), aff'd, No. 2021-2203, 2022 WL 17421225 (Fed. Cir. Dec. 6, 2022). In Blix, the asserted

claim was directed to a system that used an intermediary to relay communications between parties, allowing the parties to communicate anonymously. See Blix Inc. v. Apple, Inc., No. 19-1869, D.I. 17 at 7 (Defs. Opening Br., Feb. 12, 2020). To do this, the system assigned each party a public email address that was different from their private email address and required a "record of the relation between the two addresses so that the public address c[ould] be linked to the private address." Id.

Here, because Claim 13 is conceptually similar the claim at issue in Blix, it is also directed to an abstract idea. As provided in the SAC, like the system in Blix, the '107 Patent's "ID cloaking system 108 'serves as an intermediary between the end user's email system and the relying party's email system' to 'protect[] privacy by cloaking and de-cloaking confidential information in emails as they travel between these parties." (SAC at ¶ 60 (quoting '107 Patent, 4:6-13).) Also like the claim in Blix, the '107 Patent accomplishes this by assigning both parties to the email communication a cloaked, or public, email address that is different from their de-cloaked, or private, email address. (See id. at ¶ 56.) Finally, again like the claim in Blix, the claims in the '107 Patent describe a record keeping system, described as "the end user profile," through which the system can identify the party's de-cloaked email address associated with their cloaked address. (Id.)

Courts have held that "whether a patent's claims can be performed in the human mind or using a pencil and paper can inform whether a claim is abstract." Broadband iTV, Inc. v. Amazon.com, Inc., 113 F.4th 1359, 1367 (Fed. Cir. 2024). Here, Defendant argues that each step detailed in Claim 13 "can be performed manually, using a typical email program on an end user's computer, or simply by hand delivering notes." (Doc. No. 42 at 12.) To illustrate, Defendant provides extensive examples that pare down to two simple analogies: (1) a person agreeing to act

as an intermediary and anonymously forward emails between two parties by manually changing the "From" and "To" addresses in each email; and (2) a book publisher agreeing to receive and forward fan mail to an author in order to keep the author's address confidential. (Doc. No. 46 at 5.) While real-world analogies alone are not sufficient to make an idea abstract, these analogies demonstrating that the steps covered in Claim 13 can be performed by a human are a "telltale sign of abstraction." Broadband iTV, 113 F.4th at 1367; Trinity Info Media, LLC v. Covalent, Inc., 72 F.4th 1355, 1361-62 (Fed. Cir. 2023).

2. Alice Step Two: Claim 13 of the '107 Patent Provides an Inventive Concept

Plaintiff argues that, even if the '107 Patent is directed to an abstract idea, it is nevertheless patent-eligible under step two of the Alice paradigm. (Doc. No. 45 at 7.) Regarding the second step of the Alice framework, the relevant question is whether Claim 13 in the '107 Patent contains additional elements that amount to something "significantly more" to transform the '107 Patent into a patent-eligible application of the abstract idea. See Alice, 573 U.S. at 217-18. Plaintiff contends that Claim 13 achieves this standard because it provides an inventive concept. (Doc. No. 45 at 7.) But Defendant disagrees, asserting that, rather than containing an inventive concept, Claim 13 "[s]imply append[s] conventional steps, specified at a high level of generality," which does not make an abstract idea patentable. (Doc. No. 42 at 18 (quoting Affinity Labs I, 838 F.3d at 1259).)

To be an "inventive concept," the claim elements must "involve more than performance of well-understood, routine, [and] conventional activities previously known to the industry." Berkheimer, 881 F.3d at 1367 (internal quotations omitted). An "inventive concept can be found in the non-conventional and non-generic arrangement of known, conventional pieces." Bascom Glob. Internet Servs., 827 F.3d at 1350. But merely reciting "concrete, tangible components is

insufficient to confer patent eligibility to an otherwise abstract idea." In re TLI Comm'ns LLC Patent Litig., 823 F.3d 607, 613 (Fed. Cir. 2016). Moreover, in determining whether an inventive concept is present, courts have "repeatedly cited allegations in the complaint to conclude that the disputed claims were potentially inventive." See Cellspin Soft, Inc. v. Fitbit, Inc., 927 F.3d 1306, 1317 (Fed. Cir. 2019) (concluding "plausible and specific factual allegations that aspects of the claims are inventive are sufficient" to defeat a motion to dismiss).

Here, viewing the facts in the light most favorable to Plaintiff, the elements of Claim 13 combine to transform the claim into the inventive concept of anonymous email chain threading. Specifically, Claim 13's domain name limitations combine with its final limitation to enable the parties to anonymously maintain an email chain thread in a "unique way" that "was not conventional, routine, or well-known in the art." (See SAC at ¶ 68.) First, Claim 13's "domain name limitations" instruct the ID cloaking system to alter the domain of the relying party's email address before forwarding the email to the end user. (Doc. No. 45 at 20.) As alleged in the SAC, Claim 13 provides the following domain name limitations:

> wherein the relying party address has a different domain than the cloaked relying party email address; [and]
>
> wherein the new cloaked relying party email address is generated with a domain different than the relying party address[.]

(SAC at ¶ 57 (quoting Claim 13 of the '107 Patent).) Said differently, the first time a relying party emails a specific end user, Claim 13's domain name limitations require the ID cloaking system to generate a cloaked email for the relying party that has a different domain than its de-cloaked email address. For example, if the relying party's de-cloaked email address is "info@nordstrom.com," the ID cloaking system will generate a cloaked email address for the relying party with a different domain, such as "info@autograph.me." (See '107 Patent at 11:54-67.)

Second, Claim 13's final limitation instructs the ID cloaking system to swap the relying party's de-cloaked email address with its cloaked email address before it sends the email to the end user. (See SAC at ¶ 56.) This final limitation states: "wherein the email is configured with a reply-to email address comprising the new cloaked relying party email address." (Id.) In other words, when the ID cloaking system intercepts an email from a relying party to an end user and generates a cloaked email address for the relying party, as required by Claim 13's domain name limitations, this final limitation instructs the system to replace the relying party's de-cloaked email address in the "From" line with its cloaked email address before it forwards the email onto the end user. (See Doc. No. 45 at 19). For example, if Nordstrom emails an end user, the ID cloaking system will alter the de-cloaked "From: info@nordstrom.com" line of the email to instead read "From: info@autograph.me."

Moreover, by combining Claim 13's domain name limitations with its final limitation, these claim elements enable the parties to anonymously maintain email chain threading. If the end user decides to respond to the relying party's email, she need only hit "reply." (See SAC at ¶ 67.) Because Claim 13's domain name limitations instructed the ID cloaking system to generate the relying party a cloaked email address with a different domain and because the final limitation instructed the system to insert this new cloaked email address into the "From" line before it sent the email to the end user, the end user's "reply" email will be sent to the relying party's cloaked email address and thus intercepted by the ID cloaking system. There, the system will "intelligently" swap each party's respective cloaked and de-cloaked email addresses before forwarding the end user's reply onto the relying party's de-cloaked email.

To illustrate, if an end user using the de-cloaked email "example@gmail.com" responds to an email from "info@autograph.me," the ID cloaking system will intercept the reply email and

alter the "To: info@autograph.me" line to instead read "To: info@nordstrom.com." Similarly, it will alter the "From: example@gmail.com" line to instead read "From: example@autograph.me." With these alterations, the ID cloaking system is ensuring the end user's reply is received by the relying party by forwarding it to the relying party's de-cloaked email address, while also making sure the end user remains anonymous by changing the "From" field to reflect the end user's cloaked email address. As the SAC explains, "[b]y following the unconventional series of steps but by still maintaining the look and feel of an email chain, the user is not only able to operate the system as she usually would, but the chain provides necessary context to the communication and helps remind the user of what the communication is about. As such, the end user's sensitive information (even her real email address) never falls into the hands of the merchants or others whose use of the information may be trusted but still are susceptible to data breaches." (Id.)

Accordingly, on the limited record here and accepting the SAC's allegations as true, Plaintiff has adequately alleged that Claim 13 contains an inventive concept which sufficiently transforms the '107 Patent into a patent-eligible application of an abstract idea to survive a § 101 eligibility analysis under Rule 12(b)(6).

B. Plaintiff's Second Amended Complaint Plausibly Alleges a Patent Infringement Claim Against Defendant

Defendant next argues that Plaintiff's SAC fails to plausibly allege a patent infringement claim because it does not demonstrate that Defendant's "Hide-My-Email" product operates in the same way required by Claim 13's limitations. (Doc. No. 42 at 7.) As explained by Defendant, Claim 13 of the '107 Patent, the asserted claim, "requires the ID cloaking system to determine whether the end user profile contains a previous association with the relying party, and [to] create a new cloaked relying party address if no previous association exists." (Id. at 24.) But contrary to the asserted claim, Defendant contends that "the videos [Plaintiff] cites [in its SAC] do not show

a 'relying party' sending an email for the first time to a 'Hide-My-Email' address, much less suggest that 'Hide-My-Email' consults a user profile to determine whether there is a previous association between the end user and the relying party." (Id.) In response, Plaintiff argues it has "unquestionably [] satisfied its obligation for pleading infringement of a patent." (Doc. No. 45 at 22.)

A plaintiff alleging patent infringement "need not prove its case at the pleadings stage." Nalco Co. v. Chem-Mod, LLC, 883 F.3d 1337, 1350 (Fed. Cir. 2018) (quoting In re Bill of Lading Transmission & Processing Sys. Pat. Litig., 681 F.3d 1323, 1339 (Fed. Cir. 2012)) (internal quotations omitted). Instead, a court need only "test the sufficiency of the complaint, not [] decide the merits." Id. "A plaintiff is not required to plead infringement on an element-by-element basis." Bot M8 LLC v. Sony Corp. of Am., 4 F.4th 1342, 1352 (Fed. Cir. 2021). "Specific facts are not necessary; the statement need only 'give the defendant fair notice of what the . . . claim is and the ground upon which it rests.'" Disc Disease Solutions Inc. v. VGH Solutions, Inc., 888 F.3d 1256, 1260 (Fed. Cir. 2018) (quoting Erickson v. Pardus, 551 U.S. 89, 93 (2007)) (alteration in original).

Here, Plaintiff has sufficiently alleged a patent infringement claim against Defendant at this stage of the proceedings. Despite Defendant's arguments to the contrary, the SAC contains "an extensive description of how [Defendant's] accused 'Hide-My-Email' product . . . operates." (Doc. No. 45 at 22 (citing SAC at ¶¶ 79-88).) For example, the SAC makes the following allegations, among others, about Defendant's "Hide-My-Email" product:

> On information and belief, the ["Hide-My-Email" product] provide[s] "[a] nontransitory computer readable medium for a [sic] ID cloaking system" by operating the website https://www.Apple.com/ and providing a mobile application in order to provide privacy measures to its customers and users, including but not limited to its "Hide-My-Email" feature.
>
> On information and belief, the ["Hide-My-Email" product] "receive[s] an email addressed to a cloaked end user address, wherein the email is sent from a relying

> party email address." For example, according to Defendant, the "Hide-My-Email" product "lets you create unique, random email addresses that forward to your personal inbox so you can send and receive email without having to share your real email address."
>
> On information and belief, the ["Hide-My-Email" product] provide[s] that "the domain of the cloaked end user address and the domain associated to the cloaked ID system are the same domain." For example, according to Defendant, the "Hide-My-Email" product routes end user and relying party emails through the same intermediary computer system located at the same domain (i.e., iCloud.com).
>
> On information and belief, the ["Hide-My-Email" product] "identif[ies] an end user specified address associated to the cloaked end user address by an end user profile[.]"
>
> * * *
>
> On information and belief, the ["Hide-My-Email" product] "send[s] the email to the identified end user specified address, wherein the email is configured with a reply-to email address comprising the new cloaked relying party email address[.]"

(SAC at ¶¶ 80-83, 88 (quoting Claim 13 of the '107 Patent).)

Notably, these allegations compare Plaintiff's understanding of the inner-workings of Defendant's "Hide-My-Email" product to the Claim 13 limitations. Because Plaintiff is not required at the pleadings stage to have full knowledge of how "Hide-My-Email" works, these well-pleaded allegations drawn from Plaintiff's "information and belief" are sufficient for Plaintiff's infringement claim to survive a motion to dismiss. See DermaFocus LLC v. Ulthera, Inc., 201 F. Supp. 3d 465, 469 n.7 (D. Del. 2016) ("And, indeed, it may not be possible for a plaintiff to describe its case-in-chief with particularity at the outset of litigation, without access to the accused method, the accused apparatus for reverse engineering, or confidential data such as source code."); BioMérieux, S.A. v. Hologic, Inc., No. 18-21, 2018 WL 4603267, at *4 (D. Del. Sept. 25, 2018) ("Plaintiffs cannot be charged with knowing, at the time they drafted their Complaint, non-public information they could only obtain after filing suit and obtaining discovery. It was appropriate [at the motion to dismiss stage] for Plaintiffs here to rely on publicly-available information . . . .")

Accordingly, accepting Plaintiff's well-pleaded factual allegations as true, Plaintiff has plausibly alleged a claim for patent infringement.

V. CONCLUSION

For the foregoing reasons, Defendant's Motion to Dismiss Plaintiff's Second Amended Complaint (Doc. No. 41) will be denied. An appropriate Order follows.

IPR2024-01446
Apple, Inc. v. Rally AG LLC
Ex. 2002