UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SMART AUTHENTICATION IP, LLC,
Plaintiff,
v.
ELECTRONIC ARTS INC.,
Defendant.

Case No. 19-cv-01994-SI

ORDER GRANTING DEFENDANT'S MOTION TO DISMISS

Re: Dkt. No. 21

Before the Court is a motion to dismiss brought by defendant Electronic Arts Inc. ("EA"), which seeks a finding that U.S. Patent No. 8,082,213 (the "'213 patent") is invalid and patent-ineligible under 35 U.S.C. § 101. Dkt. No. 21 (Motion to Dismiss). This matter came on for hearing on August 9, 2019. Having read the papers and heard the parties' arguments the Court hereby GRANTS defendant's motion, finding the '213 patent invalid under § 101 and dismisses the complaint with prejudice.

BACKGROUND

On December 20, 2011, the '213 patent, entitled "Method and System for Personalized Online Security," was duly and lawfully issued by the U.S. Patent and Trademark Office. Compl. ¶ 7. Plaintiff, Smart Authentication, is the assignee and owner of the right, title and interest in and to the '213 patent. Compl. ¶ 8. The inventions of the '213 patent generally relate to methods and systems for multi-factor authentication of users over multiple communications media. Compl. ¶ 9. The '213's patent abstract states:

> Various embodiments of the present invention provide strong authentication of users on behalf of commercial entities and other parties to electronic transactions. In these embodiments of the present invention, a user interacts with an authentication service provider [“ASP”] to establish policies for subsequent authentication of the user. Thus, in these embodiments of the present invention, a user controls the level and complexity of authentication processes carried out by the authentication service provider on behalf of both the user and commercial entities and other entities seeking to authenticate the user in the course of conducting electronic transactions, electronic dialogues, and other interactions for which user authentication is needed. The policies specified by a user may include specification of variable-factor authentication, in which the user, during the course of an authentication, provides both secret information as well as evidence of control of a tangible object.

Dkt. No. 25-2 at 16 (‘213 Patent).[1] Figure 3 of the ‘213 patent provides a helpful illustration of one of the patent’s potential uses. Specifically, it models an interaction between a user, an ASP client, and an ASP. *Id.* at 5.

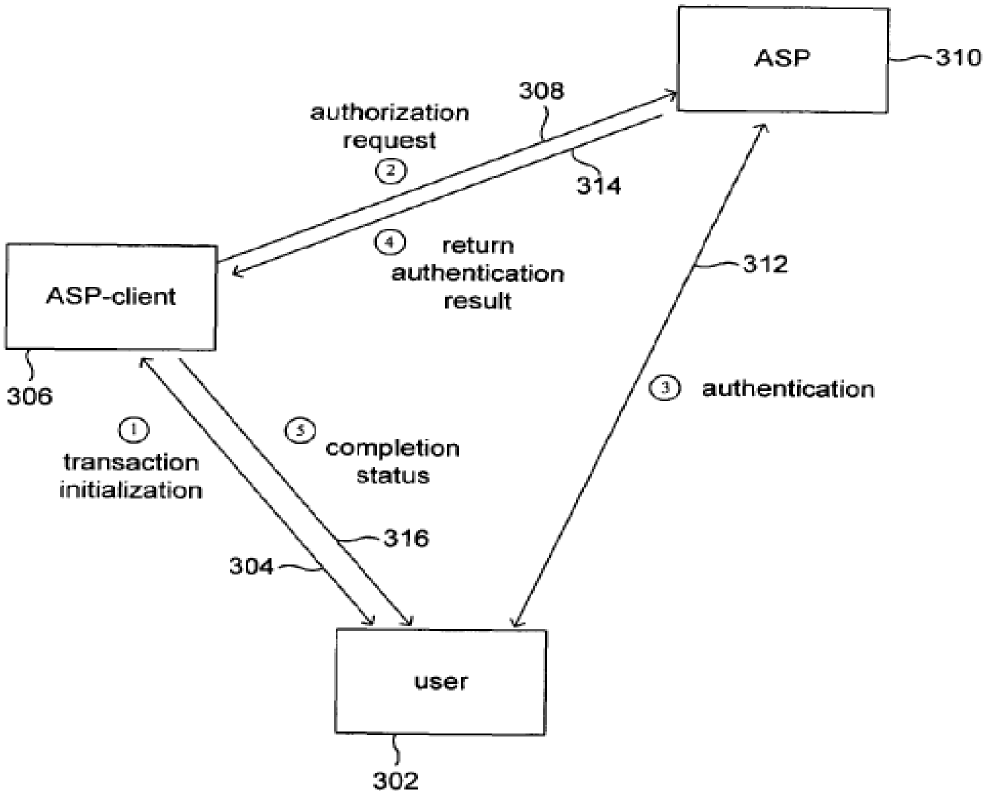

Figure 3

[1] For ease of reference, page citations to docket entries will refer to the ECF assigned page

The ‘213 patent contemplates a user trying to login to the user’s account on a website, for example. In order to strengthen the security of the user’s login credentials and protect the user’s information, the user could be prompted to select an alternative form of authorization confirmation. The user could select to confirm her authorization via a secondary medium, including, but not limited to, a text message on her cell phone or an email. The secondary authenticating medium would occur outside the purview of the initial login credentials. This second form of authentication confirms the user’s identity.

Prior to filing the instant action, Smart Authentication was engaged in proceedings before the Patent Trial and Appeal Board. Claim 11 emerged as the sole remaining claim following an *inter partes* review (IPR). Dkt. No. 21 at 10, Footnote 2 (Motion to Dismiss); see also Dkt. Nos. 25-3 and 25-4 (Decision on Appeal and Final Written Decision, respectively, attached to the Shekhar Vyas Declaration in Support of Opposition). Claim 11 is dependent upon claims 1, 9, and 10 (all of which were invalidated in the IPR). The relevant claims read:

> 1. A user-authentication service implemented as routines that execute one or more computer systems interconnected by two or more communications media with both an authentication-service client, and a user, the user-authentication service comprising:
>
> the one or more computer systems;
>
> stored user-authentication policies specified by the user;
>
> stored user information;
>
> account interface routines that implement an account interface by which the user specifies, modifies, adds, and deletes user-authentication policies; and
>
> authentication-interface routines that implement an authentication interface by which, following initiation of a transaction by the user with the authentication service client, the authentication-service client submits an authentication request, through the first communications medium or through a second communications medium, to authenticate the user, the authentication interface routines employing a variable-factor authentication, when specified to do so by stored user-authentication policies, to authenticate the user on behalf of the authentication-service client during which the user communicates with the user-authentication service through a third communications medium different from the first and second communications media and a user device different from that employed by the user to initiate the transaction with the authentication-service client.
>
> 9. The user-authentication service of claim 1 wherein a user-authentication policy specifies one or more of: constraints and parameters associated with user-

> authentication processes carried out by the user-authentication service on behalf of one or more, specified authentication-service clients.
>
> 10. The user-authentication service of claim 9 wherein constraints include one or more of:
>
> geographical constraints;
>
> time-of-day constraints;
>
> date constraints;
>
> communications -medium-related constraints;
>
> user-authentication service actions; and
>
> event constraints.
>
> 11. The user-authentication service of claim 10 wherein user-authentication service actions include one or more of:
>
> halting authorization service after detecting a specified event;
>
> employing particular types of user-authentication procedures; and
>
> providing alerts upon detecting specified events.

Dkt. No. 25-2 at 16-17 (‘213 Patent).

Plaintiff’s complaint, filed in April 2019, alleges a single cause of action for direct infringement against defendant EA. Specifically, plaintiff alleges:

> Without license or authorization and in violation of 35 U.S.C. § 271(a), Defendant is liable for infringement of claim 11 of the ‘213 patent by making, using, importing, offering for sale, selling and/or hosting a method for authenticating a user that requires two-factor authentication, including, but not limited to Login Verification, because each and every element is met either literally or equivalently.

Compl. ¶ 16.

LEGAL STANDARD

I. Motion to Dismiss

Under Federal Rule of Civil Procedure 12(b)(6), a district court must dismiss a complaint if it fails to state a claim upon which relief can be granted. To survive a Rule 12(b)(6) motion to dismiss, the plaintiff must allege “enough facts to state a claim to relief that is plausible on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). This “facial plausibility” standard requires the plaintiff to allege facts that add up to “more than a sheer possibility that a defendant has acted unlawfully." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). While courts do not require "heightened fact pleading of specifics," a plaintiff must allege facts sufficient to "raise a right to relief above the speculative level." *Twombly*, 550 U.S. at 555, 570.

To state a claim for patent infringement, "a patentee need only plead facts sufficient to place the alleged infringer on notice. This requirement ensures that the accused infringer has sufficient knowledge of the facts alleged to enable it to answer the complaint and defend itself." *Phonometrics, Inc. v. Hospitality Franchise Sys., Inc.*, 203 F.3d 790, 794 (Fed. Cir. 2000). The Federal Circuit has "repeatedly recognized that in many cases it is possible and proper to determine patent eligibility under 35 U.S.C. § 101 on a Rule 12(b)(6) motion." *Genetic Techs. Ltd. v. Merial L.L.C.*, 818 F.3d 1369, 1373 (Fed. Cir. 2016).

II. Subject Matter Eligibility Under § 101

Under 35 U.S.C. § 101, the scope of patentable subject matter encompasses "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof." *Bilski v. Kappos*, 561 U.S. 593, 601 (2010) (quoting 35 U.S.C. § 101). Section 101 "contains an important implicit exception: Laws of nature, natural phenomena, and abstract ideas are not patentable." *Alice Corp. v. CLS Bank Int'l*, 573 U.S. 208, 216 (2014) (quoting *Ass'n for Molecular Pathology v. Myriad Genetics, Inc.*, 569 U.S. 576, 589 (2013)). They are not patent-eligible because "they are the basic tools of scientific and technological work," which are "free to all men and reserved exclusively to none." *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 71 (2012) (citations omitted). The United States Supreme Court has explained that allowing patents for such purported inventions "might tend to impede innovation more than it would tend to promote it[,]" thereby thwarting the primary objective of patent laws. *Id.*

Alice provides the relevant analytical 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. First, the court must determine whether the claims at issue are directed to one of the patent-ineligible concepts. *Id.* Second, if the claims are directed to a patent-ineligible concept, such as an abstract idea, the court must "consider the elements of each

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE