UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

FAIRWARNING IP, LLC,

Plaintiff,

v. CASE NO. 8:14-cv-2685-T-23MAP

IATRIC SYSTEMS, INC.,

Defendant.
_____/

ORDER

FairWarning IP, LLC, sues (Doc. 47) Iatric Systems, Inc., for infringing United States Patent No. 8,578,500. Challenging the patent's validity, Iatric moves (Doc. 68) to dismiss under 35 U.S.C. § 101.

BACKGROUND

The '500 patent (Doc. 47-1) claims a "system and method of detecting fraud and/or misuse in a computer environment based on analyzing data." '500 patent, col. 1, ll. 15–17. Specifically, Claim 1 describes a "method of detecting improper access of a patient's protected health information . . . in a computer environment"; Claim 12 describes a "system" that implements Claim 1's method; and Claim 14 describes a "computer-readable medium" containing program code that performs Claim 1's method. '500 patent, col. 16, ll. 27–29; col. 17, l. 24; col. 18, l. 7. Also, the patent contains fourteen dependent claims (Claims 2–11, 13, and 15–17), each

of which adds a slight limitation to the method, the system, or the computer-readable medium.

According to FairWarning, "the '500 patent analyzes audit log data in order to identify potential snooping and identify theft by authorized users" of "electronic patient medical records." (Doc. 52 at 2) The '500 patent reviews each "user's activity, identity, frequency of activity, and the like," and "in appropriate circumstances a 'hit' is stored in memory and a 'notification' is provided." (Doc. 52 at 2, 11) Iatric challenges (Doc. 50) the '500 patent's validity and argues that the patent "claims the abstract idea of analyzing records of human activity to detect suspicious behavior, and its direction to 'apply it' in the computer context fails to describe an improvement to the function of a computer itself, or an improvement in another technological field." (Doc. 50 at 2)

DISCUSSION

Limiting the subject matter of a patent-eligible invention, 35 U.S.C. § 101 states, "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." Section 101 excludes from patent protection a law of nature, a natural phenomenon, and an abstract idea.

Alice Corp. v. CLS Bank International, 134 S. Ct. 2347, 2355 (2014), identifies a two-step analysis required to determine a patent's validity under Section 101:

> First, . . . determine whether the claims at issue are directed to one of those patent-ineligible concepts. If so . . . , then ask, "what else is there in the claims . . . ?" To answer that question, . . . consider the elements of each claim both individually and "as an ordered combination" to determine whether the additional elements "transform the nature of the claim" into a patent-eligible application.

Analysis under *Alice* begins by determining whether the "concept" that the patent is "directed to" or "drawn to" is a patentable concept. *Alice* considers a patent that, like the '500 patent, claims a method, a system, and a computer-readable medium. In *Alice*, 134 S. Ct. at 2352, "[t]he claims at issue relate to a computerized scheme for mitigating 'settlement risk'" through a third-party intermediary. Without "labor[ing] to delimit the precise contours of the 'abstract idea' category," *Alice*, 134 S. Ct. at 2356–57, explains that the patented "scheme" (known as "intermediated settlement") is a "fundamental" and "long prevalent" practice.

As Iatric correctly argues, the '500 patent is "directed to" or "drawn to" the concept of "analyzing records of human activity to detect suspicious behavior." (Doc. 50 at 2) Reviewing activity to detect suspicious behavior is not unique to the context of private health information, and binding precedent has invalidated patents "directed to" similar concepts. *E.g.*, *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1367 (Fed. Cir. 2011) (invalidating a patent that claimed a "method and system for detecting fraud in a credit card transaction between [a] consumer and a merchant over the Internet"); *accord Intellectual Ventures II LLC v. JP Morgan Chase & Co.*, 2015 WL 1941331, *3 (S.D.N.Y. April 28, 2015) (Hellerstein, J.) (invalidating a patent that claimed a "method for monitoring multiple computer hosts within a network for

anomalies, and alerting the various hosts of possible intrusion"); *Wireless Media Innovations, LLC v. Maher Terminals, LLC*, 2015 WL 1810378, *8 (D.N.J. April 20, 2015) (Linares, J.) (invalidating patents "directed to the . . . abstract idea[of] monitoring locations, movement, and load status of shipping containers within a container-receiving yard, and storing, reporting and communicating this information in various forms through generic computer functions"). Reviewing activity to detect suspicious behavior is a basic and well-established abstract idea.[1]

Attempting to demonstrate that the '500 patent is not "directed to" an abstract idea, FairWarning analogizes to *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1257 (Fed. Cir. 2014), which upholds a patent in which the "claims address[] the problem of retaining website visitors that, if adhering to the routine, conventional functioning of Internet hyperlink protocol, would be instantly transported away from a host's website after 'clicking' on an advertisement and activating a hyperlink." Finding that the patent comports with Section 101, the Federal Circuit stated that the patent "do[es] not merely recite the performance of some business practice known from the pre-Internet world along with the requirement to perform it on the Internet." *DDR Holdings*, 773 F.3d at 1258. "Instead, the claimed solution is necessarily rooted in computer technology in order to overcome a problem specifically arising in the

[1] Also, Iatric argues that the '500 patent's "claims do little more than mirror [the Health Information Portability and Accountability Act] regulations" and that, therefore, the claims are "directed to" a "conventional (and indeed even required) activity in the industry." (Doc. 50 at 17, 19) Because this order invalidates the '500 patent, Iatric's argument that "[p]atenting compliance with HIPAA regulations obviously threatens to pre-empt the field" (Doc. 50 at 17) remains unresolved.

realm of computer networks." *DDR Holdings*, 773 F.3d at 1258. In other words, no "pre-Internet analog of the patent's asserted claims" exists because the problem addressed by claims is unique to "the realm of computer networks." *DDR Holdings*, 773 F.3d at 1257, 1258.

In a strained comparison, FairWarning argues that the '500 patent "provides a solution to a technological problem, namely, identifying potential snooping and identity theft by authorized users." (Doc. 52 at 10) However, *DDR Holdings* is inapposite because the '500 patent is not "necessarily rooted in computer technology." FairWarning asserts that "analyzing audit log data is not like analyzing human behavior, as audit log data examines the electronic footprint or trail of activities that are executed in a computer environment." (Doc. 52 at 7) But, as Iatric states, the '500 patent "is but a modern spin" (Doc. 50 at 16) on reviewing activity to detect suspicious behavior, an activity that existed in the "pre-Internet world."[2]

The '500 patent is "directed to" an abstract idea; therefore, the second *Alice* step applies. The second *Alice* step requires an examination of "the elements of the claim to determine whether it contains an 'inventive concept' sufficient to 'transform' the claimed abstract idea into a patent-eligible application." *Alice*, 134 S. Ct. at 2357. A successful transformation requires "more than simply stating the abstract idea while adding the words 'apply it.'" *Alice*, 134 S. Ct. at 2357.

---

[2] Even if FairWarning could identify a meaningful distinction between reviewing "audit log data" and analyzing human behavior, as *DDR Holdings*, 773 F.3d at 1258, cautions, "not all claims purporting to address Internet-centric challenges are eligible for patent." *DDR Holdings*, 773 F.3d at 1258, explains that the patent cannot "broadly and generically claim 'use of the Internet' to perform an abstract business practice (with insignificant added activity)."

1. Claims 1–11

Claim 1 of the '500 patent, the patent's "representative" method, states:

> 1. A method of detecting improper access of a patient's protected health information (PHI) in a computer environment, the method comprising:
>
> generating a rule for monitoring audit log data representing at least one of [the] transactions or activities that are executed in the computer environment, which are associated with the patient's PHI, the rule comprising at least one criterion related to accesses in excess of a specific volume, accesses during a pre-determined time interval, accesses by a specific user, that is indicative of improper access of the patient's PHI by an authorized user wherein the improper access is an indication of potential snooping or identity theft of the patient's PHI, the authorized user having a pre-defined role comprising authorized computer access to the patient's PHI;
>
> applying the rule to the audit log data to determine if an event has occurred, the event occurring if the at least one criterion has been met;
>
> storing, in a memory, a hit if the event has occurred; and
>
> providing notification if the event has occurred.

'500 patent, col. 16, ll. 27–46.

In other words, Claim 1 comprises (1) generating a rule "related to" the number of accesses, the timing of accesses, and the specific users in order to review "transactions or activities that are executed in a computer environment"; (2) applying the rule; (3) storing the result; and (4) announcing the result. None of these steps necessarily requires the use of a computer or any other technology. Rather, a person using "the human mind, or . . . using a pen and paper," *CyberSource Corp.,* 654 F.3d at 1372, can generate a rule for reviewing "audit log data" (i.e., a record of

activity) based on specific criteria, can apply the rule, can record the result, and can announce the result. Because the human mind can perform each step, Claim 1's method is unpatentable. *CyberSource Corp.,* 654 F.3d at 1373 ("[C]omputational methods which can be performed entirely in the human mind are the types of methods that embody the basic tools of scientific and technological work that are free to all men and reserved exclusively to none." (internal quotation marks omitted)); *see also Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat. Ass'n*, 776 F.3d 1343, 1347 (Fed. Cir. 2014) (invalidating patents that claimed a method of extracting data from documents, recognizing specific information, and storing that information in a memory because "the concept of data collection, recognition, and storage is undisputedly well-known" and "humans have always performed these functions").

None of the steps in Claim 1's method transforms the abstract idea into a patentable concept. Although the first step of the method requires "generating a rule for monitoring audit log data," Claim 1 neither states a rule nor instructs a computer to generate a rule. Instead, in at least one embodiment of the invention, "the rule is created by the user and/or a third party, such as a consultant with particular knowledge as to fraud or misuse of the particular type of data." '500 patent, col. 13, ll. 11–13. Also, the function performed by the computer in each remaining step of Claim 1's method is "purely conventional." *Alice*, 134 S. Ct. at 2358. Using a computer to apply a rule is elemental computing — the most basic

function of a computer. Similarly, using a computer to record a result and to announce a result are "well-understood, routine, conventional activities previously known to the industry." *Alice*, 134 S. Ct. at 2359 (internal quotation marks omitted).

Even considered as "an ordered combination," the steps of Claim 1's method add "nothing significantly more than an instruction to apply the abstract idea . . . using some unspecified, generic computer." *Alice*, 134 S. Ct. at 2360. In other words, "[t]his ordered combination of steps recites an abstraction — an idea, having no particular concrete or tangible form." *Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 709, 715 (Fed. Cir. 2014). Thus, the steps of the method are not "'enough' to transform an abstract idea into a patent-eligible invention." *Alice*, 134 S. Ct. at 2360.

Further, none of Claim 1's dependent claims adds a meaningful limitation to bring the abstract idea within the scope of Section 101. For example, Claim 2 adds "normalizing" or formatting the data; Claim 3 adds obtaining an authorized user's "role information"; and Claims 4, 5, and 6 add tracking an authorized user's access, volume of access, and time of access.

Finally, the abstract idea remains unpatentable despite the patent's effort to limit the invention to one field (health information) and to one technology (a computer). *See Bilski v. Kappos*, 561 U.S. 593, 612 (2010) ("[L]imiting an abstract idea to one field of use or adding token postsolution components d[oes] not make [a] concept patentable."); *Accenture Global Servs., GmbH v. Guidewire Software, Inc.*, 728 F.3d 1336, 1345 (Fed. Cir. 2013) (invalidating under Section 101 a patent despite

the patent's "attempt[] to limit the abstract concept to a computer implementation and to a specific industry").

2. Claims 12 and 13

Claim 12, which describes a system that implements on a generic computer Claim 1's method, is not patentable. Like the system in *Alice*, the system in Claim 12 contains a "handful of generic components." Specifically, Claim 12's system comprises an "interface" and a "microprocessor," both of which are fundamental components of every computer. "As a result, none of the hardware recited by the system claims offers a meaningful limitation beyond generally linking the use of the method to a particular technological environment, that is, implementation via computers." *Alice*, 134 S. Ct. at 2360 (internal quotation marks omitted).

Thus, Iatric correctly argues that "[t]he patent tethers an abstract idea — analyzing records to detect suspicious behavior — to a general purpose computer, a classic example of patent ineligibility under Section 101." (Doc. 50 at 11) Because the system adds no meaningful limitation to the method, Claim 12 is unpatentable for the same reasons as Claim 1. Similarly, Claim 13, a dependent claim that contains the additional limitation of "tracking access by the authorized user," is not an inventive concept that renders Claim 12 patentable.

3. Claims 14–17

Claim 14, which describes a computer-readable medium that contains instructions to perform Claim 1's method, fails for the same reasons. The patent states

that the computer-readable medium "can be any available media which can be accessed by a general purpose or special purpose computer," such as "RAM, ROM, EPROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices." '500 patent, col. 15, ll. 30–36. The patent's invocation of generic computer-readable media to perform the method adds no inventive concept to the underlying abstract idea. *See CyberSource Corp.*, 654 F.3d at 1375 (finding that the use of a computer-readable medium to verify credit card transactions and to detect fraud is an unpatentable abstract idea). None of Claim 14's dependent claims compels a different result.

CONCLUSION

Iatric's motion (Doc. 50) for oral argument is **DENIED**. Iatric's motion (Doc. 50) to dismiss is **GRANTED**, and the complaint is **DISMISSED WITHOUT PREJUDICE**. Under Section 101, the '500 patent is invalid. No later than **JULY 9, 2015**, FairWarning may amend the complaint to assert a claim that is independent of the '500 patent's validity. If FairWarning fails to amend the complaint on or before July 9, 2015, an order will promptly dismiss this action with prejudice.

ORDERED in Tampa, Florida, on June 24, 2015.

STEVEN D. MERRYDAY
UNITED STATES DISTRICT JUDGE