UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/014,584	01/26/2011	Ben Dominguez	79900-797103(060110US)	1917

66945 7590 03/30/2018

KILPATRICK TOWNSEND & STOCKTON LLP/VISA
Mailstop: IP Docketing - 22
1100 Peachtree Street
Suite 2800
Atlanta, GA 30309

EXAMINER
RANKINS, WILLIAM E

ART UNIT	PAPER NUMBER
3694	

NOTIFICATION DATE	DELIVERY MODE
03/30/2018	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ipefiling@kilpatricktownsend.com
EDurrell@kilpatricktownsend.com
KTSDocketing2@kilpatrick.foundationip.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte BEN DOMINGUEZ, JAGDEEP SAHOTA, and THANIGAIVEL ASHWIN RAJ

Appeal 2017-000951
Application 13/014,584[1]
Technology Center 3600

Before BRADLEY W. BAUMEISTER, SHARON FENICK, and PHILLIP A. BENNETT, *Administrative Patent Judges*.

BENNETT, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134(a) from the Examiner's final rejection of claims 1, 3–7, 9, 11–17, 19–21, 26, 30, and 32. Claims 2, 8, 10, 18, 22–25, 27–29, 31, and 33–36 have been cancelled. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

---

[1] Appellants' Brief ("App. Br.") identifies Visa International Service Association as the real party in interest. App. Br. 3.

CLAIMED SUBJECT MATTER

The claims are directed to authenticating participants in a transaction. Spec., Abstract. Claim 1, reproduced below, is illustrative of the claimed subject matter:

> 1. An article of manufacture comprising a non-transitory computer readable storage medium storing thereon a set of instructions which when executed by a processor of a server in a computer network cause the server to:
>
> receive, by the server in the computer network, a transaction information for a money transfer transaction involving a participant, wherein the participant is a sender or a recipient in the money transfer transaction, wherein the transaction information includes a participant account identifier and one or more elements of identifying data associated with the participant;
>
> generate, by the server in the computer network, a hash value based upon providing the one or more elements of identifying data as an input to a hash algorithm, wherein the one or more elements of identifying data are not recoverable from the hash value;
>
> send, by the server in the computer network, an authorization request for the money transfer transaction to an authentication control server of an issuer of the participant account, the authorization request including the participant account identifier and the hash value but not including the one or more elements of identifying data;
>
> receive, by the server in the computer network, an authorization response from the authentication control server, the authorization response including an indicator for authenticating the participant, which is generated by the authentication control server that indicates whether one or more participant data elements stored by the authentication control server match the one or more elements of identifying data of the received transaction information by comparing the hash value in the authorization request with a computed hash value computed by the authentication control sever based on the one or more

> participant data elements stored by the authentication control server; and
>
> authorize, by the server in the computer network, the money transfer transaction when the indicator indicates that the one or more participant data elements stored by the authentication control server match the one or more elements of identifying data of the received transaction information, and that the participant is authenticated.

App. Br. 19 (Claims Appendix).

REJECTION

Claims 1, 3–7, 9, 11–17, 19–21, 26, 30 and 32 stand rejected under 35 U.S.C. § 101 as being directed to patent-ineligible subject matter. Final Act. 3–6.

OPINION

Examiner's Findings and Conclusion of Ineligibility

In rejecting the claims under 35 U.S.C. § 101, the Examiner concludes the claims are directed to the abstract idea of "authorization of a money transfer transaction" by "generating a hash value." Final Act. 3, 5. The Examiner finds the abstract idea to which the claims are directed is similar to concepts previously found ineligible by courts, such as that concept found ineligible by the Supreme Court in *Gottschalk v. Benson*, 409 U.S. 63 (1972). Further explaining his determination, the Examiner states:

> Money transfer transactions are not necessarily rooted in computer technology. With the proliferation of computers money transfers by computer have become commonplace[,] but they are not necessary. Authorization of money transfers is also

> not necessarily completed by computers[,] but computers have been used to automate the authorization process.

Final Act. 3.

The Examiner also determines the claims do not amount to significantly more than the abstract idea because the limitations recited in the claims are conventional data processing operations, and they do not add "a specification limitation other than what is well-understood, routine and conventional in the field, or add[] unconventional steps that confine the claim to a particular useful application." Final Act. 6.

Appellants' Contentions

Appellants assert several errors in the Examiner's analysis. With respect to the Examiner's determination that the claims are directed to an abstract idea, Appellants first argue *Benson* is not on point because "the present claims recite much more than just a hash value, and include a specific practical and useful application of the hash value." App. Br. 11–12 (identifying various limitations in claim 1 additional to those reciting the use of hashing). Appellants argue these limitations "provide a practical application of using the hash value—namely to authenticate a participant for authorization of a transaction," and they do not present the preemption concerns present in *Benson*. App. Br. 12.

Next, Appellants argue the pending claims should be found eligible based on the analysis set forth in the in our non-precedential decisions in *PNC Bank. v. Secure Axcess, LLC*, CBM2014-00100 (PTAB Sept. 9, 2014) and *NRT Tech. Corp. v. Everi Payments, Inc.*, CBM2015-00167 (PTAB January 22, 2016). *Id*; *see also* Reply Br. 6–8 (citing additional non-precedential decisions).

In their Reply Brief, Appellants further contend the Examiner's characterization of the claims oversimplifies the nature of the invention and is untethered from the language of the claims contravening the Federal Circuit's admonition in *Enfish* and *McRO*. Reply Br. 4. Appellants argue the "Examiner did not consider the specific requirements of the claims such as the authentication of a participant for authorization of a transaction conducted over a network, or that the identifying data is not sent with the hash value, or that the identifying data is not recoverable from the hash value, etc." Reply Br. 4–5.

Appellants also advance arguments disputing the Examiner's finding that the claims do not amount to significantly more than the abstract idea. Appellants rely primarily on *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245 (Fed Cir. 2014), arguing that its claims are analogous to those found eligible in that case. App. Br. 13–14. In particular, Appellants contend "one of the problems addressed by the claims is to authenticate a participant of a transaction over an insecure network such as the Internet." App. Br. 14. Appellants argue this problem arises only in the context of computer networks and that the claimed invention solves the problem through its use of hash values to protect identifying information. *Id.* Appellants further argue the claims provide "significantly more" than the abstract idea because the specific hash value generated in the claims is more secure and prevents compromise of sensitive information. App. Br. 15–16. Finally, Appellants contend the use of hashing to avoid sending sensitive identifying information in the context of a money transfer transaction request is unconventional to what has been previously done as evidenced by the lack of cited prior art. App. Br. 17.

Legal Standard for Patent Eligibility

In issues involving subject matter eligibility, our inquiry focuses on whether the claims satisfy the two-step test set forth by the Supreme Court in *Alice Corp. v. CLS Bank Int'l*, 134 S. Ct. 2347 (2014). The Supreme Court instructs us to "first determine whether the claims at issue are directed to a patent-ineligible concept," *Alice*, 134 S. Ct. at 2355, and, in this case, the inquiry centers on whether the claims are directed to an abstract idea. If the initial threshold is met, we then move to the second step, in which we "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." *Id.* (*quoting Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 79, 78 (2012)). The Supreme Court describes the second step as a 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.'" *Id.* (quoting *Mayo*, 566 U.S. at 72–73).

Analysis

Here, the Examiner characterizes the invention as being directed to the abstract idea of "authorization of a money transfer transaction" by "generating a hash value." Final Act. 3, 5. This characterization is supported by the evidence. For example, Appellants' Specification describes the invention as addressing "the need to ensure the security and reliability of transactions" and that "embodiments of the disclosure are directed to systems and method for authenticating various identification attributes of a participant in a transaction." Spec. ¶¶ 2, 8. Further, the

Specification states that this security and reliability is achieved by converting the identifying information in the transaction to an encoded value using well-known hash algorithms. Spec. ¶ 56. These descriptions in the Specification are consistent with the Examiner's characterization of the invention to which the claims are directed, and we discern no error in this determination.

As we noted above, Appellants argue the claims are not directed to an abstract idea because they are dissimilar to those found ineligible by the Supreme Court in *Benson*—providing a practical use which mitigates any concerns of preemption. This argument is not persuasive because courts have held that lack of preemption is not dispositive of the abstract idea inquiry. *Ariosa Diagnostics, Inc. v. Sequenom, Inc.*, 788 F.3d 1371, 1379 (Fed. Cir. 2015) ("While preemption may signal patent ineligible subject matter, the absence of complete preemption does not demonstrate patent eligibility.").

Moreover, Appellants' claims are more similar to those claims found to be abstract and ineligible in prior cases. For example, in *Elec. Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350 (Fed. Cir. 2016) the Federal Circuit found the claims abstract because their focus was "on collecting information, analyzing it, and displaying certain results of the collection and analysis." *Id.* at 1353. Here, similarly, the claims focus on a process by which a money transfer, a process previously performed manually without the benefit of computers, is effectuated by receiving, modifying, transmitting, and comparing data in order to provide authorization for the transfer. In other cases, the Federal Circuit "ha[s] made clear that mere automation of manual processes using generic computers does not constitute

a patentable improvement in computer technology." *Credit Acceptance Corp. v. Westlake Servs.*, 859 F.3d 1044, 1055 (Fed. Cir. 2017) (internal citation omitted). Appellants' claims automate the process of transferring money between two parties, a process that prior to the advent of computers and computer networks was carried out manually. As such, "the focus of the claims is not on such an improvement in computers as tools, but on certain independently abstract ideas that use computers as tools." *Id.*

We also do not find persuasive Appellants' argument that the claims address a problem unique to computer networks in the same manner as the claims in *DDR Holdings*. Authentication of participants in money transfer transaction is not a new problem. Nor is it unique to the Internet, as banks have long required persons to show identification to conduct banking business.

Finally, we do not agree with Appellants that the use of a hash algorithm recited in the claim constitutes an improvement in computer technology similar to that leading to patent-eligibility in *Enfish*. Rather, as we discuss in more detail in our *Alice* step 2 analysis below, in light of Appellants' acknowledgement in the Specification that the use of the hash algorithms was known (Spec. ¶ 56), we view the use of a hash algorithm not as an improvement to computer technology, but instead as application of the computer as a tool to implement the abstract idea. *Credit Acceptance Corp.*, 859 F.3d at 1055.

Turning to the second step of the *Alice/Mayo* analysis, we agree with the Examiner that the steps carried out in Appellants' claims amount only to the use of conventional data processing operations in carrying out the abstract idea. Appellants' Specification acknowledges the bulk of the

money transfer process is conventional. For example, the Specification states that "[e]mbodiments of the disclosure extend the 3-D Secure authentication protocol and framework to include authentication of identification details." Spec. ¶ 31. By indicating the invention merely extends the existing, conventional 3-D Secure protocol, the Specification acknowledges that much of the claimed process involves the use of conventional and well-known technologies which effectuate a money transfer transaction.

Appellants emphasize that the claims offer "significantly more" than the abstract idea because they protect underlying identifying data "by sending a hash value generated from identifying data but not sending the identifying data themselves." App. Br. 15. However, the Federal Circuit has found that hash values are not sufficient to transform a patent-ineligible concept into something more. *Smart Sys. Innovations, LLC v. Chi. Transit Auth.*, 873 F.3d 1364, 1374 (Fed. Cir. 2017) (finding the use of hash identifiers fails to provide an inventive concept under *Alice* step 2).

Moreover, the Specification also acknowledges that the use of hash values to protect data was conventional. For example, the Specification states that "[w]ith a properly designed hash algorithm, the original data used to calculate the hash value cannot be recovered from the hash value," and that "[t]he creation of such hash algorithms is known in the art." Spec. ¶ 56. Still further, the Specification provides no details or teaching regarding how to design or otherwise implement such a hash algorithm, further underscoring the fact that their use was well-known and conventional.

Nor are we persuaded by Appellants' argument that the lack of any prior art rejections demonstrates the claim implementation is not routine and

conventional. Appellants essentially argue that because the claims are not shown to be unpatentable over the prior art of record, the claims cannot be well-known and conventional under the Alice/Mayo framework. This argument lacks merit because it presupposes that any claim found to be novel and non-obvious over prior art cannot be an abstract idea within the *Alice/Mayo* framework.

We are aware of no case supporting this proposition, nor do Appellants cite to any. Rather, patent-eligibility under 35 U.S.C. § 101 is a threshold requirement that must be satisfied *in addition to* being novel, nonobvious, and fully and particularly described. *See Bilski v.* Kappos, 561 U.S. 593, 602 (2010). Appellants' proffered rule would not make sense, as it would limit the application of 35 U.S.C. § 101 to only those claims found to be otherwise unpatentable under other sections of the Patent Act (e.g., 35 U.S.C. §§ 102, 103). In short, a finding of novelty or non-obviousness does not necessarily lead to the conclusion that subject matter is patent-eligible. "Groundbreaking, innovative, or even brilliant discovery does not by itself satisfy the § 101 inquiry." *Ass'n for Molecular Pathology v. Myriad Genetics, Inc.*, 133 S. Ct. 2107, 2117 (2013).

Accordingly, we are not persuaded the Examiner has erred in determining Appellants' claims do not amount to significantly more than the abstract idea, and we sustain the rejection under 35 U.S.C. § 101.

DECISION

We affirm the Examiner's rejection of claims 1, 3–7, 9, 11–17, 19–21, 26, 30, and 32.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a). *See* 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED