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.
13/360,537	01/27/2012	Janet Smith	21652-00178	8496

75564 7590 03/27/2019
DANIEL M. FITZGERALD (21652)
ARMSTRONG TEASDALE LLP
7700 Forsyth Boulevard
Suite 1800
St. Louis, MO 63105

EXAMINER	
KAZIMI, HANI M	

ART UNIT	PAPER NUMBER
3691	

NOTIFICATION DATE	DELIVERY MODE
03/27/2019	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):

USpatents@armstrongteasdale.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte JANET SMITH, JOHN D. CHISHOLM, JOHAN GERBER,
CLARA SALAZAR, MATTHEW WICKMAN, SUSAN MEYER,
RACHAEL VAHLE CORDERO, and CHRISTOPHER JOHN MERZ

Appeal 2018-001726
Application 13/360,537[1]
Technology Center 3600

Before JUSTIN BUSCH, CARL L. SILVERMAN, and
JAMES W. DEJMEK, *Administrative Patent Judges*.

DEJMEK, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants appeal under 35 U.S.C. § 134(a) from a Final Rejection of claims 1–24. We have jurisdiction over the pending claims under 35 U.S.C. § 6(b).

We affirm.

[1] Appellants identify MasterCard International Incorporated as the real party in interest. App. Br. 1.

STATEMENT OF THE CASE

Introduction

Appellants' disclosed and claimed invention generally relates to "providing fraud risk scoring of payment card transactions including card-not-present (CNP) transactions." Spec. ¶ 2. According to the Specification, a fraud risk score provides an indication of the likelihood that the transaction on the associated card account is fraudulent. Spec. ¶ 51. In a disclosed embodiment, a fraud risk score may be determined by using at least one of a plurality of fraud scoring models. Spec. ¶ 53. A fraud scoring model may be selected based on predetermined criteria such as an issuing region associated with the payment card account. Spec. ¶ 53. The scoring model also uses a payment card account profile associated with the payment card used in the transaction. Spec. ¶ 54. According to the Specification, the payment card account profile may contain historical transaction information as well as "long term variables," which collect spending behaviors over a defined time period. Spec. ¶¶ 54–55.

Claim 1 is representative of the subject matter on appeal and is reproduced below:

> 1. A fraud detection computer system comprising:
>
> a network host site;
>
> an interchange network comprising a processor communicatively coupled to a memory device for storing data and to said network host site, said processor programmed to:
>
> > store a payment card account profile in the memory device, wherein the payment card account profile is associated with a payment card account, and wherein the payment card account profile includes one or more long term variables representing a spending behavior for card-present and card-not-present transactions over a

predetermined and selectable time period for the payment card account;

store a plurality of fraud scoring models at said network host site, wherein each of the plurality of fraud scoring models is configured to generate a fraud risk score by applying a fraud scoring algorithm to the one or more long term variables;

receive, from a merchant, a card transaction authorization request message that includes transaction data for a card-not-present (CNP) transaction, fraud scoring model selection criteria, and a fraud risk score request indicator representing an instruction by the merchant to score the CNP transaction for fraud risk, wherein the transaction data includes a primary account number (PAN) for the payment card account, and the fraud scoring model selection criteria include one or more of: (i) an issuing region associated with the CNP transaction and (ii) a subscription status of the merchant and an issuer of the payment card;

convert the PAN into a hashed PAN value using a secure hash algorithm (SHA), wherein the hashed PAN value is of a predetermined digest size;

load, into the plurality of fraud scoring models, the hashed PAN value and the one or more long term variables, wherein the one or more long term variables are loaded as a single comma-delimited line;

select at least one fraud scoring model of the plurality of fraud scoring models, based on the fraud scoring model selection criteria;

calculate the fraud risk score for the CNP transaction using the at least one fraud scoring model;

transmit the card transaction authorization request message to the issuer of the payment card for approval of the card transaction authorization request; and

route a card transaction authorization request response message received from the issuer to the

> merchant, wherein the card transaction authorization request response message includes an issuer authorization decision received from the issuer and the fraud risk score.

The Examiner's Rejection

Claims 1–24 stand rejected under 35 U.S.C. § 101 as being directed to patent-ineligible subject matter. Final Act. 2–5.

ANALYSIS[2]

Appellants dispute the Examiner's conclusion that the pending claims are directed to patent-ineligible subject matter. App. Br. 6–14; Reply Br. 1–4. In particular, Appellants argue the Examiner oversimplifies the claims and overlooks specific requirements of the claims that "go far beyond the alleged abstract idea of 'providing fraud risk scoring of payment card-not-present (CNP) transactions.'" App. Br. 7–8 (quoting Final Act. 3); Reply Br. 1–2. For example, Appellants assert storing a plurality of fraud scoring models for selection based on the issuing region associated with the transaction card account or the inclusion of historical transaction information for a payment card account "provides a much richer fraud score to the merchants." App. Br. 9. Thus, rather than being directed to an abstract idea, Appellants argue the claims are directed to "a specific implementation of a solution to a problem in the software arts." App. Br. 7–10 (discussing *McRO, Inc. v. Bandai Namco Games Am. Inc.*, 837 F.3d 1299, 1314 (Fed.

[2] Throughout this Decision, we have considered the Appeal Brief, filed July 5, 2017 ("App. Br."); the Reply Brief, filed December 6, 2017 ("Reply Br."); the Examiner's Answer, mailed October 6, 2017 ("Ans."); and the Final Office Action, mailed December 30, 2016 ("Final Act."), from which this Appeal is taken.

Cir. 2016) and *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1336 (Fed. Cir. 2016)); Reply Br. 2–3. Appellants further argue the benefits of the claimed invention come not from merely executing mathematical equations on a generic computing platform, but, rather, by applying specific rules to the approach. App. Br. 10. Moreover, Appellants assert the claims recite "significantly more" than the alleged abstract idea to transform the alleged abstract idea into a patent-eligible application. App. Br. 11–13; Reply Br. 3–4. Specifically, Appellants assert the claimed invention is "necessarily rooted in computer technology—detection of fraud inherent in an electronic payment network that enables card-based transactions to occur without the cardholder being present." App. Br. 12–13; Reply Br. 3–4 (citing *BASCOM Global Internet Servs. v. AT&T Mobility LLC*, 827 F.3d 1341 (Fed. Cir. 2016)).

The Supreme Court's two-step framework guides our analysis of patent eligibility under 35 U.S.C. § 101. *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. 208, 217 (2014). In addition, the Office recently published revised guidance for evaluating subject matter eligibility under 35 U.S.C. § 101, specifically with respect to applying the *Alice* framework. USPTO's 2019 Revised Patent Subject Matter Eligibility Guidance, 84 Fed. Reg. 50 (Jan. 7, 2019) ("Office Guidance"). If a claim falls within one of the statutory categories of patent eligibility (i.e., a process, machine, manufacture, or composition of matter) then the first inquiry is whether the claim is directed to one of the judicially recognized exceptions (i.e., a law of nature, a natural phenomenon, or an abstract idea). *Alice*, 573 U.S. at 217. As part of this inquiry, we must "look at the 'focus of the claimed advance over the prior art' to determine if the claim's 'character as a whole' is directed to excluded subject matter." *Affinity Labs of Tex., LLC v. DirecTV, LLC*, 838 F.3d 1253, 1257–58 (Fed. Cir. 2016) (internal citations omitted). Per Office Guidance, this first inquiry has two prongs of analysis: (i) does the claim recite a judicial exception (e.g., an abstract idea), and (ii) if so, is the judicial exception integrated into a practical application. 84 Fed. Reg. at 54. Under the Office Guidance, if the judicial exception is integrated into a practical application, *see infra*, the claim is eligible under § 101. 84 Fed. Reg. at 54–55. If the claim is directed to a judicial exception (i.e., recites a judicial exception and does not integrate the exception into a practical application), the next step is to determine whether any element, or combination of elements, amounts to significantly more than the judicial exception. *Alice*, 573 U.S. at 217; 84 Fed. Reg. at 56.

Here, we conclude Appellants' claims recite an abstract idea of a mental process. In particular, Appellants' claims are generally directed to calculating a fraud risk score for a card-not-present (CNP) transaction, i.e., an evaluation that may be performed in the human mind. *See* Spec. ¶ 21 ("Embodiments . . . relate to determining a fraud risk score in payment card transactions, such as, card-not-present payment card transactions."); *see also* App. Br. 6–7. Consistent with our Office Guidance and case law, we conclude that calculating a fraud risk score for a CNP transaction is a mental process—i.e., an abstract idea. *See* 84 Fed. Reg. at 52; *see also CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1371–72 (Fed. Cir. 2011) (concluding claims directed to "detecting credit card fraud based on information relating to past transactions" can be performed in the human mind and were drawn to a patent-ineligible mental process); *FairWarning IP, LLC v. Iatric Sys., Inc.*, 839 F.3d 1089, 1093–94 (Fed. Cir. 2016) (concluding claims directed to "collecting and analyzing information to detect misuse and notifying a user when misuse is detected" to be mental processes within the abstract-idea category).

Claim 1is reproduced below and includes the following claim limitations that recite calculating a fraud risk score for a card-not-present (CNP) transaction, emphasized in *italics*.

> 1. A fraud detection computer system comprising:
>
> a network host site;
>
> an interchange network comprising a processor communicatively coupled to a memory device for storing data and to said network host site, said processor programmed to:
>
> > store a payment card account profile in the memory device, wherein the payment card account profile is associated with a payment card account, and wherein the payment card account profile includes one or more long term variables representing a spending behavior for card-present and card-not-present transactions over a predetermined and selectable time period for the payment card account;
> >
> > store a plurality of fraud scoring models at said network host site, wherein each of the plurality of fraud scoring models is configured to generate a fraud risk score by applying a fraud scoring algorithm to the one or more long term variables;
> >
> > *receive, from a merchant, a card transaction authorization request message that includes transaction data for a card-not-present (CNP) transaction, fraud scoring model selection criteria, and a fraud risk score request indicator representing an instruction by the merchant to score the CNP transaction for fraud risk, wherein the transaction data includes a primary account number (PAN) for the payment card account, and the fraud scoring model selection criteria include one or more of: (i) an issuing region associated with the CNP*

> *transaction and (ii) a subscription status of the merchant and an issuer of the payment card;*
>
> *convert the PAN into a hashed PAN value using a secure hash algorithm (SHA), wherein the hashed PAN value is of a predetermined digest size;*
>
> *load, into the plurality of fraud scoring models, the hashed PAN value and the one or more long term variables, wherein the one or more long term variables are loaded as a single comma-delimited line;*
>
> *select at least one fraud scoring model of the plurality of fraud scoring models, based on the fraud scoring model selection criteria;*
>
> *calculate the fraud risk score for the CNP transaction using the at least one fraud scoring model;*
>
> transmit the card transaction authorization request message to the issuer of the payment card for approval of the card transaction authorization request; and
>
> route a card transaction authorization request response message received from the issuer to the merchant, wherein the card transaction authorization request response message includes an issuer authorization decision received from the issuer and the fraud risk score.

More particularly, calculating a fraud risk score for a card-not-present (CNP) transaction comprises: (i) receiving the relevant transaction data and identifying the desired fraud risk model to be used (i.e., the claimed steps of receiving a card authorization request message and selecting a fraud risk score model based on the content of the received message); and (ii) calculating the fraud risk score (i.e., the claimed steps of securely converting the account number to a determined size, loading the relevant data into the selected fraud score model, and calculating the fraud risk score).

Because the claim recites a judicial exception, we next determine whether the claim integrates the judicial exception into a practical application. 84 Fed. Reg. at 54. To determine whether the judicial exception is integrated into a practical application, we identify whether there are "*any additional elements recited in the claim beyond the judicial exception(s)*" and evaluate those elements to determine whether they integrate the judicial exception into a recognized practical application. 84 Fed. Reg. at 54–55 (emphasis added); *see also* Manual of Patent Examining Procedure (MPEP) § 2106.05(a)–(c), (e)–(h) (9th ed. Rev. 08.2017, Jan. 2018).

Here, we find the additional limitations do not integrate the judicial exception into a practical application. More particularly, the claims do not recite: (i) an improvement to the functionality of a computer or other technology or technical field (*see* MPEP § 2106.05(a)); (ii) use a "particular machine" to apply or use the judicial exception (*see* MPEP § 2106.05(b)); (iii) a particular transformation of an article to a different thing or state (*see* MPEP § 2106.05(c)); or (iv) any other meaningful limitation (*see* MPEP § 2106.05(e)). *See also* 84 Fed. Reg. at 55. Specifically, (i) storing a payment card account profile; (ii) storing a plurality of fraud scoring models; (iii) transmitting the card transaction authorization request message to the payment card issuer; and (iv) routing a response message comprising an authorization decision and the calculated fraud risk score merely recite the type of extra-solution activities (i.e., in addition to the judicial exception) the courts have determined insufficient to transform judicially excepted subject matter into a patent-eligible application. *See* MPEP § 2106.05(g); *see also* *Bilski v. Kappos*, 561 U.S. 593, 612 (holding the use of well-known techniques to establish inputs to the abstract idea as extra-solution activity that fails to make the underlying concept patent eligible); *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1355 (Fed. Cir. 2016) (explaining that "selecting information, by content or source, for collection analysis, and display does nothing significant to differentiate a process from ordinary mental processes"); *Elec. Power*, 830 F.3d at 1354 (recognizing "that merely presenting the results of abstract processes of collecting and analyzing information, without more (such as identifying a particular tool for presentation), is abstract as an ancillary part of such collection and analysis"); *Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 709, 716 (Fed. Cir. 2014) (determining "the steps of consulting and updating an activity log represent insignificant data-gathering steps") (internal quotation omitted); *Bancorp Servs, L.L.C. v. Sun Life Assur. Co. of Can.*, 771 F.Supp.2d 1054, 1065 (E.D. Mo. 2011) *aff'd*, 687 F.3d 1266 (Fed. Cir. 2012) (explaining that "storing, retrieving, and providing data . . . are inconsequential data gathering and insignificant post solution activity").

Additionally, we disagree with Appellants (*see* App. Br. 7) that, as a whole, the claims are directed to a specific implementation of a solution to a problem in the software arts. Unlike the claims in *Enfish*, the instant claims are not focused on an improvement to computers as tools, but rather use computers to execute the judicial exception. *See* Ans. 6; *see also Credit Acceptance Corp. v. Westlake Servs.*, 859 F.3d 1044, 1055 (Fed. Cir. 2017).

In *DDR Holdings*, the Federal Circuit explained that the patent-eligible claims specified "how interactions with the Internet are manipulated to yield a desired result . . . that overrides the routine and conventional sequence of events ordinarily triggered by the click of a hyperlink." *DDR*

Holdings, 773 F.3d at 1258. The court reasoned that those claims recited a technological solution "necessarily rooted in computer technology" that addressed a "problem specifically arising in the realm of computer networks." *DDR Holdings*, 773 F.3d at 1257. In contrast, Appellants acknowledge in the Specification that fraud detection may be performed by various techniques including "manually flagging and checking high risk orders." Spec. ¶ 4. Thus, the problem does not arise specifically in the realm of computer networks or the software arts.

Moreover, in *BASCOM*, the court found "the patent describes how its particular arrangement of elements is a technical improvement," and, when construed in favor of BASCOM,[3] the claims may be read to improve an existing technological process. *BASCOM*, 827 F.3d at 1350. We disagree with Appellants (*see* Reply Br. 4) that moving fraud scoring models from merchant systems to a network host system represents an unconventional arrangement of elements sufficient to confer patent eligibility. Appellants suggest such an arrangement provides for a different fraud model to be selected based upon certain criteria. Reply Br. 4. However, the Specification does not describe why desired fraud scoring models could not be hosted on merchant systems, or other technical concerns that are addressed by moving the plurality of fraud scoring models to a network host.

For at least the foregoing reasons, the claims do not integrate the judicial exception into a practical application.

Because we determine the claims are directed to an abstract idea or combination of abstract ideas, we analyze the claims under step two of *Alice*

[3] In *BASCOM*, BASCOM appealed the district court's granting of a motion to dismiss under Fed. R. Civ. P. 12(b)(6). *BASCOM*, 827 F.3d at 1341.

to determine if there are additional limitations that individually, or as an ordered combination, ensure the claims amount to "significantly more" than the abstract idea. *Alice*, 573 U.S. at 217–18 (citing *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 72–73, 77–79 (2012)). As stated in the Office Guidance, many of the considerations to determine whether the claims amount to "significantly more" under step two of the *Alice* framework are already considered as part of determining whether the judicial exception has been integrated into a practical application. 84 Fed. Reg. at 56. Thus, at this point of our analysis, we determine if the claims add a specific limitation, or combination of limitations, that is not well-understood, routine, conventional activity in the field; or simply append well-understood, routine, conventional activities at a high level of generality. 84 Fed. Reg. at 56.

Here, Appellants' claims do not recite specific limitations (or a combination of limitations) that are beyond what was well-understood, routine, and conventional. As an initial matter, we note, as does the Examiner (*see, e.g.*, Ans. 8), Appellants describe the components of the claimed invention at a high level of generality and the components perform generic functions that are well-understood, routine, and conventional. *See* Spec. ¶¶ 30–33, 40–50, 72–72, Figs. 4, 5. For example, transmitting the card authorization request to the payment card issuer or routing a card authorization request response message from the payment card issuer to the merchant via a communication interface does not amount to "significantly more" than the judicial exception. *See buySAFE, Inc. v. Google, Inc.*, 765 F.3d 1350, 1355 (Fed. Cir. 2014) ("That a computer receives and sends the information over a network—with no further specification—is not even arguably inventive."). Similarly, storing data (i.e., either payment card account profiles or a plurality of fraud scoring models) in memory is a generic function of a workstation (i.e., computer) located at a network host site. *See Alice*, 573 U.S. at 226 at 2360 ("Nearly every computer will include a 'communications controller' and a 'data storage unit' capable of performing the basic calculation, storage, and transmission functions required by the method claims."); *Content Extraction & Transmission v. Wells Fargo Bank, N.A.*, 776 F.3d 1343, 1348 (Fed. Cir. 2014) ("storing information" into memory and using a computer to "translate the shapes on a physical page into typeface characters" are insufficient to confer patent eligibility); *Mortgage Grader, Inc. v. First Choice Loan Servs. Inc.*, 811 F.3d 1314, 1324–25 (Fed. Cir. 2016) (generic computer components, such as an "interface," "network," and "database," fail to satisfy the inventive concept requirement).

Additionally, to the extent Appellants contend the claims do not seek to tie-up an abstract idea (App. Br. 13), we are unpersuaded of Examiner error. "'[W]hile preemption may signal patent ineligible subject matter, the absence of complete preemption does not demonstrate patent eligibility.'" *FairWarning IP*, 839 F.3d at 1098 (quoting *Ariosa Diagnostics, Inc. v. Sequenom, Inc.*, 788 F.3d 1371, 1379 (Fed. Cir. 2015); *see also OIP Techs., Inc. v. Amazon.com, Inc.*, 788 F.3d 1359, 1362–63 (Fed. Cir. 2015) ("[T]hat the claims do not preempt all price optimization or may be limited to price optimization in the e-commerce setting do not make them any less abstract."). Further, "[w]here a patent's claims are deemed only to disclose patent ineligible subject matter under the *Mayo* framework, as they are in this case, preemption concerns are fully addressed and made moot." *Ariosa*, 788 F.3d at 1379.

For the reasons discussed *supra*, we are unpersuaded of Examiner error. Accordingly, we sustain the Examiner's rejection of claims 1–24 under 35 U.S.C. § 101.

DECISION

We affirm the Examiner's decision rejecting claims 1–24 under 35 U.S.C. § 101.

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. § 41.50(f) (2016).

AFFIRMED