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.
15/239,657	08/17/2016	Scott Michael Zoldi	35006-784F01US	5643

76615 7590 09/11/2020
Mintz Levin/Fair Isaac
Mintz Levin Cohn Ferris Glovsky and Popeo, P.C.
One Financial Center
Boston, MA 02111

EXAMINER	
NORMAN, SAMICA L	

ART UNIT	PAPER NUMBER
3697	

NOTIFICATION DATE	DELIVERY MODE
09/11/2020	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):

IPDocketingBOS@mintz.com
IPFileroombos@mintz.com
mintzdocketing@cpaglobal.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte SCOTT MICHAEL ZOLDI and HEMING XU

Appeal 2020-002863
Application 15/239,657
Technology Center 3600

Before ULRIKE W. JENKS, TAWEN CHANG, and
MICHAEL A. VALEK, *Administrative Patent Judges.*

CHANG, *Administrative Patent Judge.*

DECISION ON APPEAL

Pursuant to 35 U.S.C. § 134(a), Appellant[1] appeals from the Examiner's decision to reject claims 1–18. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM.

[1] We use the word "Appellant" to refer to "applicant" as defined in 37 C.F.R. § 1.42. Appellant identifies the real party in interest as Fair Issac Corporation. Appeal Br. 3.

STATEMENT OF THE CASE

As described in the Specification,

> [u]nderstanding the spending patterns of customers is crucial to rapidly detect fraudulent transactions so as to mitigate monetary losses for both card issuers and merchants. The spending patterns are established based upon customer's behavior in the aspects of spending time, merchant location, purchase amount and merchant category code (MCC) etc. The patterns may be extracted from the ever-growing volume of the historical transaction data with a variety of techniques. The cardholder historical data include all the attributes of transactions involving customers and merchants and transaction types etc. One technique is to examine the customer spending history in large databases and then dividing customers into different subsets based on their spending characteristics of transactions. The underlying assumption may be that the consumers in the same subset may have similar behaviors or characteristics.

Spec. ¶ 3.

CLAIMED SUBJECT MATTER

The claims are directed to methods to detect and systems for detecting fraudulent transactions. Claim 1 is illustrative:

> 1. A method to detect fraudulent transactions comprising:
>
> [(a)] receiving, by a merchant transaction computer during a card-not-present (CNP) online transaction conducted over a communications network, data representing a new transaction from a customer's payment card,
>
> [(b)] associating, by the merchant transaction computer, the customer with an archetype distribution stored in an electronic database, the archetype distribution being generated by an archetype calculation engine based on past transactions across a plurality of merchants by the customer and customer attributes and computed by an issuer or processor of the customer's payment card;
>
> [(c)] generating, by the archetype calculation engine, a topic model based on one or more words and/or one or more documents selected from the data representing the new transaction and the past transactions, the topic model

representing a similarity of the words and/or documents of the new transaction with words and/or documents in the past transactions represented by the archetypes;

[(d)] generating, by the archetype calculation engine, archetype clusters based on archetype distribution vectors for each document upon execution of the topic model, the archetype clusters representing a similarity of documents in the archetype space based on past transactions by the customer and customer attributes;

[(e)] associating, by the merchant transaction computer, the customer with an archetype cluster generated by the archetype cluster calculation engine based on data representing the past transactions from the customer or one or more other customers, the archetype cluster representing a distribution of a probability of attributes related to each of the past transactions at the merchant;

[(f)] locating, by the merchant transaction computer from the electronic database, an archetype distribution vector and the archetype cluster generated by the archetype calculation engine based on data representing the past transactions from the customer or one or more other customers, the archetype cluster representing a distribution of a probability of attributes related to each of the past transactions at a multitude of merchants, the archetype distribution vector representing the current archetype distribution of the customer's transactions across the multitude of merchants;

[(g)] generating, by the merchant transaction computer in near real time to the CNP transaction, a first score representing a likelihood of fraud associated with the new transaction based on the calculated transaction risks associated with global archetype cluster membership, merchant-specific archetype cluster membership, and recurrence list positions of transaction details;

[(h)] generating, by the merchant transaction computer using a frequent-behavior sorted list method, a second score based on a frequency of transactions associated with the customer, the frequent behavior sorted list method comprising generating a frequency table including non-fraudulent and

> fraudulent activity in different merchant-specific archetype clusters;
>
> [(i)] calculating, by the merchant transaction computer, a risk score based on a weighted sum of the first score and the second score;
>
> [(j)] determining, in response to the risk score exceeding a preset threshold, that the new transaction is fraudulent;
>
> [(k)] performing, in response to the determining, an action on the new transaction, and
>
> [(l)] updating the topic model and the frequency table with the new transaction.

Appeal Br. 22–23 (Claims App.) (annotations added).

REJECTION

Claims 1–18 are rejected under 35 U.S.C. § 101 as being directed to an abstract idea without significantly more.

OPINION

A. Issue

The Examiner concludes that "[t]he claimed limitations, under its broadest reasonable interpretation, are **based upon** mathematical relations, formulations or calculations and a fundamental economic principles or practice," which are abstract ideas and thus fall within one of the judicial exceptions to patent eligibility. Ans. 3. In addition, the Examiner finds that "[t]h[ese] judicial exception[s are] not integrated into a practical application," because the additional elements (i.e., "an archetype calculation engine (software) and a merchant transaction computer") do not use the mathematical calculations and fundamental economic practice in a sufficiently specific manner. *Id.* at 4. The Examiner further finds that "[t]he claims do not include additional elements that are sufficient to amount to significantly more than the judicial exception." *Id.*

Appellant contends that claim 1 is at most "based on or involves a mathematical concept" and, thus, does not ***recite*** "a mathematical relationship, a mathematical formula or equation, or a mathematical calculation" under Prong One of Step 2A of the PTO's 2019 Revised Patent Subject Matter Eligibility Guidance ("Revised Guidance"). Appeal Br. 13 (citing PTO's October 2019 Patent Eligibility Guidance Update ("Guidance Update")). Appellant further contends that "[c]laim 1 is directed to a 'method to detect fraudulent transactions[,] which is not an enumerated fundamental economic principle or practice and is not included in the examples of MPEP 2106.04." *Id.* at 14.

Appellant further contends that any abstract idea recited in claim 1 is integrated into a practical application, because claim 1 provides an improvement to a technology or technical field, e.g., "fraud detection in a network." Appeal Br. 15–16.

Finally, Appellant contends that, "[e]ven assuming, *arguendo*, that Claim 1 is directed to an abstract idea . . ., Claim 1 recites significantly more than the alleged abstract idea[s]," because "Claim 1 describes the unconventional solution (enhanced fraud detection) of using the claimed technique to solve a technical problem of providing risk scores using temporal behavior maps." Appeal Br. 17–19.

Appellant does not separately argue the claims. We therefore focus our analysis on claim 1 as representative. The issue with respect to this rejection is whether claim 1 is directed towards an abstract idea, without significantly more.

B. Analysis

We analyze this case under the framework the Supreme Court set forth in *Mayo Collaborative Services v. Prometheus Laboratories, Inc.*, 566 U.S. 66 (2012) and applied in *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. 208 (2014). As the Supreme Court explained in *Alice*:

> In *Mayo* . . . , we set forth a framework for distinguishing patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of those concepts. First, we determine whether the claims at issue are directed to one of those patent-ineligible concepts. . . . If so, we then ask, "[w]hat else is there in the claims before us?" . . . To answer that question, we consider the elements of each claim both individually and "as an ordered combination" to determine whether additional elements "transform the nature of the claim" into a patent-eligible application. . . . We have described step two of this analysis 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."

Alice, 573 U.S. at 217–218.

Whether Claim 1 Is Directed to Patent-Ineligible Concept

We begin with the first step of the *Mayo* test, namely whether a claim is "directed to" a patent-ineligible concept. On January 7, 2019, the Director of the USPTO issued the "2019 Revised Patent Subject Matter Eligibility Guidance" ("Revised Guidance"), which provides further details regarding how the Patent Office analyzes patent-eligibility questions under 35 U.S.C. § 101. 84 Fed. Reg. 50–57 (Jan. 7, 2019). Under the Revised Guidance, the first step of the *Mayo* test (i.e., Step 2A of the Revised Guidance) is "a two-pronged inquiry." *Id.* at 54. In prong one, we evaluate whether the claim recites a judicial exception, such as laws of nature, natural phenomena, or abstract ideas. *Id.* If the claim recites a judicial exception, the claim is further analyzed under prong two, which requires "evaluat[ion of] whether the claim recites additional elements that integrate the exception into a practical application of that exception." *Id.* The Revised Guidance explains that, "[i]f the recited exception is integrated into a practical application of the exception, then the claim is eligible at Prong Two of . . . Step 2A [of the Revised Guidance]." *Id.*

Prong One of Step 2A of Revised Guidance

Following the Revised Guidance, we first consider whether claim 1 recites a judicial exception such as an abstract idea.

Courts have held that patent-ineligible abstract ideas include certain methods of organizing human activity, such as fundamental economic practices, commercial or legal interactions, and managing personal behavior or relationships or interactions between people. *See, e.g., Alice*, 573 U.S. at 219–20; *Bilski v. Kappos*, 561 U.S. 593, 611 (2010). Likewise, "[m]athematical concepts – mathematical relationships, mathematical formulas or equations, mathematical calculations" – are abstract ideas that fall within the judicial exceptions to patent-eligibility. *SAP America, Inc. v. InvestPic, LLC*, 898 F.3d 1161, 1163 (Fed. Cir. 2018) (holding that claims to a ''series of mathematical calculations based on selected information'' are directed to abstract ideas); *Digitech Image Techs., LLC v. Elecs. for Imaging, Inc.*, 758 F.3d 1344, 1350 (Fed. Cir. 2014) (holding that claims to a ''process of organizing information through mathematical correlations'' are directed to an abstract idea). Finally, abstract ideas also include mental processes, including subject matter that covers performance in the mind but for the recitation of generic computer components. *Gottschalk v. Benson*, 409 U.S. 63, 69 (1972); *Mortg. Grader, Inc. v. First Choice Loan Servs. Inc.*, 811 F.3d 1314, 1324 (Fed. Cir. 2016) (holding that computer-implemented method for "anonymous loan shopping" was an abstract idea because it could be "performed by humans without a computer).

We find that the steps of claim 1, collectively as an ordered combination, recite a method of organizing human activity similar to other concepts that have been identified by the courts as abstract. *See, e.g., FairWarning IP, LLC v. Iatric Systems, Inc.*, 839 F.3d 1089, 1093 (Fed. Cir. 2016) (holding claims "'directed to or drawn to the concept of analyzing records of human activity to detect suspicious behavior'" to be directed to an abstract idea).

In particular, claim 1 on appeal is similar to the claims at issue in *Bilski* and *Alice*, in that it is directed to a computer-implemented method for carrying out a process that was widespread long before computers, the Internet, and electronic commerce: i.e., determining the likelihood that a transaction is fraudulent based on comparison with past transactions of an individual and similarly situated individuals. Detecting fraudulent transactions falls within, at least, commercial interactions such as sales activities. 84 Fed. Reg. at 52 (identifying commercial interactions including sales activities as falling within "[c]ertain methods of organizing human activity" categorized as abstract ideas).

The steps performed by the computer-readable program code of claim 1 correspond to the electronic versions of:

- "receiving . . . new transaction from a customer's payment card" (step (a));

- categorizing the customer based on data relating to (1) customer attributes; (2) attributes of the current transaction, and (3) attributes of past transactions of the customer and one or more other customers at a plurality of merchants, including the merchant receiving new transaction (steps (b)–(f)):
    - “associating . . . the customer with an archetype distribution . . . based on past transactions across a plurality of merchants by the customer and customer attributes” (step (b));
    - “generating . . . a topic model based on one or more words and/or . . . documents . . . from . . . new and past transactions, the topic model representing a similarity of the words and/or documents of the new transaction with words and/or documents in the past transactions represented by the archetypes” (step (c));
    - “generating . . . archetype clusters based on archetype distribution vectors for each document upon execution of the topic model, the archetype clusters representing a similarity of documents in the archetype space based on past transactions by the customer and customer attributes” (step (d));
    - “associating . . . the customer with an archetype cluster . . . based on . . . the past transactions from the customer or one or more other customers, the archetype cluster representing a distribution of a probability of attributes

related to each of the past transactions at the merchant" (step (e));

- "locating . . . an archetype distribution vector and the archetype cluster . . . based on . . . past transactions from the customer or one or more other customers, the archetype cluster representing a distribution of a probability of attributes related to each of the past transactions at a multitude of merchants, the archetype distribution vector representing the current archetype distribution of the customer's transactions across the multitude of merchants" (step (f));

- determining the risk that the transaction is fraudulent based on fraud risk associated with customer's membership in particular customer categories and attributes of the current transaction and the customer's past transactions:
    - "generating . . . a first score representing a likelihood of fraud associated with the new transaction based on the calculated transaction risks associated with global archetype cluster membership, merchant-specific archetype cluster membership, and recurrence list positions of transaction details" (step (g));
    - "generating . . . a second score based on a frequency of transactions associated with the customer, the frequent behavior sorted list method comprising generating a frequency table including non-fraudulent and fraudulent

    - activity in different merchant-specific archetype clusters" (step (h));
    - "calculating . . . a risk score based on a weighted sum of the first score and the second score" (step (i));
- "determining, in response to the risk score exceeding a preset threshold, that the new transaction is fraudulent" (step (j));
- "performing, in response to the determining, an action on the new transaction" (step (k)); and
- updating the relevant datasets with the new transaction (i.e., "updating the topic model and the frequency table with the new transaction" (step (l)).

In addition to reciting a method of organizing human activity, we note that claim 1 steps also recites steps that may be performed entirely in the human mind. For instance, under the broadest reasonable interpretation, step (a) recites receiving information; steps (b)–(f) recite evaluating, generating, and/or categorizing information; and steps (g)–(j) recites assessing, and making a determination based on, information, which are all actions that can be performed in the mind. 84 Fed. Reg. at 52 (identifying mental processes as a category of abstract ideas). Likewise, under the broadest reasonable interpretation, steps (b)–(i), drawn in whole or in part to generating or calculating steps, recite mathematical concepts. *Id.*

Prong Two of Step 2A of Revised Guidance

Although claim 1 recites an abstract idea, it would still be patent-eligible if "the claim as a whole integrates the recited judicial exception into a practical application of the exception"; i.e., whether the claim "appl[ies], rel[ies] on, or use[s] the judicial exception in a manner that imposes a meaningful limit on the judicial exception." 84 Fed. Reg. at 54. This analysis includes "[i]dentifying whether there are any additional elements recited in the claim beyond the judicial exception(s)" and "evaluating those additional elements individually and in combination to determine whether they integrate the exception into a practical application." *Id.* at 54–55.

In this case, the additional elements recited in claim 1 beyond the judicial exceptions are (1) "a merchant transaction computer," (2) "a card-not-present (CNP) online transaction conducted over a communications network," (3) "an electronic database," and 4) "an archetype calculation engine." Thus, other than the limitations reciting the abstract idea, the invention is claimed at a very high level of generality.

In particular, most of the additional elements the claim recites are only generic hardware and/or software elements (i.e., "transaction computer," "communications network," "electronic database," and "calculation engine"). Moreover, the recited functions performed by these elements – "receiving . . . data"; "associating" objects (e.g., associating customer and archetype distribution or archetype cluster); organizing data into particular forms (e.g., "generating" archetype distributions, topic models and archetype clusters based on customer attributes and current and past transactions, and "calculating" probabilities such as "likelihood of fraud" and "risk score"); and "updating" information – are all conventional functions of a computer.

Thus, claim 1 essentially implements an abstract idea on a computer, which does not suffice to integrate the abstract idea into a practical application. 84 Fed. Reg. at 55; *see also buySAFE, Inc. v. Google, Inc.*, 765 F.3d 1350, 1355 (Fed. Cir. 2015) (stating that "[t]he Court in *Alice* made clear that a claim directed to an abstract idea does not move into section 101 eligibility territory by 'merely requir[ing] generic computer implementation'") (alteration in original).

Likewise, "an additional element [that] adds insignificant extra-solution activity to the judicial exception" or "does no more than generally link the use of a judicial exception to a particular technological environment or field of use" does not integrate a judicial exception into a practical application. 84 Fed. Reg. at 55. The "card-not-present (CNP) online transaction" limitation recited in claim 1 does not integrate a judicial exception into a practical application, because it merely link the use of the recited abstract ideas, discussed above, to a particular type of transaction or field of use and/or add insignificant extra-solution activity to the judicial exception by providing the data needed for the performance of the abstract idea. *Id.*; *see also CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1370 (Fed. Cir. 2011) (explaining that "mere '[data-gathering] step[s] cannot make an otherwise nonstatutory claim statutory'").

In summary, claim 1 recites an abstract idea and does not integrate the abstract idea into a practical application. Therefore, claim 1 is directed to an abstract idea.

Whether Claim 1 Amounts to "Significantly More"

Finally, the Revised Guidance directs us to consider whether claim 1 includes "additional elements . . . [that] provide[] 'significantly more' than the recited judicial exception." 84 Fed. Reg. at 56. The Revised Guidance states that an additional element that "simply appends well-understood, routine, conventional activities previously known in the industry, specified at a high level of generality, to the judicial exception, . . . is indicative that an inventive concept may not be present." *Id*.

Here, as discussed, the only elements recited in claim 1, other than the abstract idea itself, are generic computer components (i.e., "a merchant transaction computer," "a communications network," "an electronic database," and "an archetype calculation engine") and "a card-not-present (CNP) online transaction conducted over [the] communications network."

The Specification further makes clear that all of these elements used to implement the invention may be generic and are thus well-understood, routine, and conventional. For instance, the Specification states that

> various aspects or features [of the subject matter described herein] can include implementation in one or more computer programs that are executable and/or interpretable on a programmable system including at least one programmable processor, which can be special or general purpose, coupled to receive data and instructions from, and to transmit data and instructions to, a storage system, at least one input device, and at least one output device.

Spec. ¶ 74; *see also id.* ¶¶ 9, 75–77. The Specification states that "[m]erchant losses [due to fraud] occur mainly on the card-not-present (CNP) transactions on the web according to the fraud statistics," which indicates that such transactions are well-understood, routine, and conventional. *Id.* ¶ 4.

In short, the additional elements of claim 1, individually or in combination, only require using a generic computer system and the Internet to perform routine communication and analysis functions, and "the mere recitation of a generic computer cannot transform a patent-ineligible abstract idea into a patent-eligible invention." *Alice*, 573 U.S. at 223. Thus, the combination of elements recited in claim 1 does not amount to significantly more than the judicial exception itself, and under 35 U.S.C. § 101 the claim is ineligible for patenting.

Appellant's Arguments

Appellant argues that, under a broadest reasonable interpretation of the claims in light of the Specification, claim 1 does not recite an abstract idea. Appellant first argues that claim 1 does not recite a fundamental economic principle or practice, because "[a]ccording to the 2019 PEG, '**fundamental economic principles or practices' include hedging, insurance, and mitigating risk and 'describe subject matter relating to the economy and commerce**,'" whereas "[c]laim 1 is directed to a 'method to detect fraudulent transactions' which is not an enumerated fundamental economic principle or practice and is not included in the examples of MPEP 2106.04." Appeal Br. 14; *see also* Reply Br. 8–11, 17. Appellant further appears to argue that, because "not a single user or person is involved in the recited steps," claim 1 "does not recite a method of organizing human activity for at least falling outside the enumerated subgroupings." Reply Br. 10–11.

We are not persuaded. As an initial matter, a claim does not need to explicitly recite a user or a person in order for the claim to recite a method of organizing human activity. For example, the claim in *Alice*, which the Supreme Court held to be directed to a fundamental economic principle or practice, also does not explicitly recite any user or person in its steps. *Alice*, 573 U.S. at 213 n. 2, 219. As the *Alice* court explained, "mere recitation of a generic computer cannot transform a patent-ineligible abstract idea into a patent-eligible invention." *Id.* at 223. The fact that claim 1 cites computers, rather than a user or person, as performing its steps, therefore, does not render the claim non-abstract.

Indeed, as already discussed above, we find that claim 1 recites a method of organizing human activity constituting an abstract idea, at least because the claim recites commercial interactions such as sales activities. The first step of claim 1, for example, recites part of a sales activity, i.e., "receiving, by a *merchant transaction* computer during a card-not-present (CNP) *online transaction* conducted over s communications network, data representing a *new transaction* from a *customer's payment card*." Appeal Br. 22 (Claims App (emphasis added).). The remaining steps recite a method for determining whether such sales activity involves a fraudulent transaction.

Appellant similarly argues that, while claim 1 may be "**based on or involves a mathematical concept**," it does not recite such a concept because it does not recite "a mathematical relationship, a mathematical formula, or a mathematical calculation." Appeal Br. 13; *see also* Reply Br. 7–8, 17.

We are not persuaded. Appellant points to the examples of mathematical relationships provided in the Guidance Update – e.g., "a ratio between force and area, a relationship between a reaction rate and a temperature, and a conversion between binary coded decimal and pure binary numerals" – and contends that "[c]laim 1 does not recite any of these examples nor describes a mathematical relationship, a mathematical formula or equation, or a mathematical calculation." Reply Br. 7.

As the Guidance Update makes clear, however, no particular words need to be used when reciting mathematical concepts, and a mathematical relationship expressed in words rather than mathematical symbols are nevertheless abstract. Guidance Update 3–4. In this case, steps (b) through (i) are all directed to generating models of, computing, and/or calculating either (1) the relationship between a current transaction and/or a customer and a larger dataset of past transactions and/or customers or (2) the likelihood of fraud associated with a particular transaction. These steps recite mathematical concepts because, as with the claims found ineligible in *Digitech Image Techs., LLC v. Elecs. for Imaging, Inc.*, 758 F.3d 1344, 1350 (Fed. Cir. 2014), they "employ[] mathematical algorithms to manipulate existing information to generate additional information." *Id.* at 1351. Step (e), for instance, describes generation of an archetype cluster that "represent[s] a *distribution of a probability* of attributes related to each of the past transactions at the merchant." Appeal Br. 22 (Claims App.) (emphasis added). Similarly, the Specification describes step (j), "calculating . . . a risk score based on a weighted sum of the first score and the second score," in terms of a mathematical formula:

$$logodds(R) = a * logoddds(R_a) + (1 - a) * logodds(R_f),$$

where a ($0<a<=1$) and ($1 - a$) represent two coefficients weighting on the two risks in *logodds* space. Spec. ¶¶ 61–62.

Appellant argues that the outputs of the process recited in claim 1 "have real-life practical applications – an ability to receive real-time feedback regarding a likelihood of fraud for a new transaction." Appeal Br. 14–15. Appellant argues that claim 1 integrates any recited abstract idea into a practical application, because, "just as the network monitors analyze specific network traffic data and generate reports to improve computer network technology in *SRI* [*International, Inc. v. Cisco Systems, Inc.*, 930

F.3d 1295 (Fed. Cir. 2019)], the merchant transaction computer of Claim 1 analyzes specific transaction data and generates scores to improve a technology (e.g., fraud detection in a network)." *Id.* at 15–16; *see also* Reply Br. 8 (analogizing claim 1 to the claims in *SRI*), 12. Appellant contends that claim 1 provides "a specific and detailed process to improve fraud detection," "imposes a meaningful limit on the alleged judicial exception," and, "like the claims in *SRI* and *DDR* [*Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245 (Fed. Cir. 2014)], prevent the normal, expected operation of conventional computer networks, namely, by detecting and stopping **fraudulent (e.g., suspicious) network activity.**" Reply Br. 10, 12, 17.

We are not persuaded. As the Supreme Court has explained, in order for a process to be patent-eligible, it must be the implementation of the abstract idea, not merely the abstract idea itself, that provide the improvement. *Parker v. Flook*, 437 U.S. 584, 594–95 (1978) (holding that a claim that provides a "new and presumably better method for calculating alarm limit values" is not patent-eligible where the only novel feature was the mathematical formula (i.e., abstract idea)). As discussed further below, any improvement to fraud detection resulting from claim 1 is provided by the abstract idea, i.e., the method of organizing human activity and the mathematical algorithms recited in claim 1, not by the implementation of these abstract ideas.

We also find Appellant's reliance on *SRI* and *DDR Holdings* to be inapposite. The claims in *SRI International* were directed to a specific improvement in *computer* functionality – "providing a network defense system that monitors network traffic in real-time to automatically detect large-scale attacks." 930 F.3d at 1303. Similarly, in *DDR Holdings* the claims "do 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"; "[i]nstead, the claimed solution is necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks." 773 F.3d at 1257. In contrast, both credit card fraud and using historical transaction data to detect fraud are known from the pre-Internet world. Spec. ¶ 2 (stating that, "[d]espite the convenience afforded by . . . credit cards, transaction security is still a tremendous task" and that "[t]he Falcon® model, one of the prominent fraud models, has been successfully developed upon the historical cardholder transaction data for [fraud detection]"). Likewise, the Specification acknowledges that "examin[g] the customer spending in large databases and then dividing customers into different subsets based on their spending characteristics of transactions" was a well understood and conventional technique employing "commonly used algorithms." Spec. ¶ 3. Thus, claim 1 does not provide an improvement with regard to how the *computers* function – instead, as discussed further below, the claimed solution at most improve fraud detection merely by combining data and algorithms used to detect fraud.

Appellant argues that the invention of claim 1 solves the problems of higher fraud rate for card not present (CNP) transactions and the limited transaction data possessed by individual merchant "by combining risk factors associated with card not present (CNP) transactions," wherein "the claimed 'aggregated measure of risk may combine the benefits from the two important risk factors: archetype-related and frequency-day (BLIST model) related.'" Appeal Br. 16. Appellant contends that the combination of the benefits from the two risk factors distinguishes the claimed technique from prior art techniques. Reply Br. 11. Appellant contends that "[t]he improvement occurs in the specific calculations of data and limitations in the claims which provide a new ability to combine benefits of two network monitoring techniques (e.g. archetype-related and frequency-related) to new transactions in a network," wherein "the method limits the processing to specific calculations and analysis to generate a determined score that allows improved predictive capability and fraud detection." Reply Br. 12.

In the Reply Brief, Appellant further argues that the claims set forth a "technology-based solution . . . for addressing the technical problems that are endemic to conventional fraud detection in card-not-present (CNP) transactions," which "allows **computer performance of a function not previously performable by a computer** (e.g., fraud detection based on archetype cluster membership and a frequency of transactions associated with a customer) as evidenced by the claimed subject matter being new and inventive under 35 U.S.C. §102 and §103." Reply Br. 5. Appellant similarly argues that, "[s]imilar to claim 1 of *Ancora Technologies*[*v. HTC America, Inc.*, 908 F.3d 1343 (Fed. Cir. 2018)], the claims in the present application address a technological problem with computers to improve security by using the specific technique of stopping fraudulent (abnormal) transactions based on a score." *Id.* at 11.

We are not persuaded. A prior art rejection is not required in order to support a rejection under § 101. Appellant essentially argues that claim 1 provides a new and improved mathematical algorithm or formula for determining whether a transaction is fraudulent. As discussed above, however, it is the claim limitations *in addition to* the abstract idea, whether individually or in combination, that must provide the improvement in the functioning of a computer or other technology or technical field when the claim is considered as a whole. 84 Fed. Reg. at 55; *see also Flook*, 437 U.S. at 594–595.

Appellant's citation to *Ancora Technologies* is inapposite. The claim at issue in *Ancora* recites "[a] method of restricting software operation within a license for use with a computer including an erasable, non-volatile memory area of a BIOS of the computer, and a volatile memory area." *Ancora Technologies*, 908 F.3d at 1345–1346. The Federal Circuit found that the claimed method is not directed to an abstract idea because it "improve[ed] security – . . . against a computer's unauthorized use of a program – . . . by specific technique that departs from earlier approaches to solve a specific computer problem." *Id.* at 1348. In this case, the problem the claim purports to solve – i.e., credit card fraud – is not a computer or Internet-specific problem,[2] and the recited solution – i.e., calculating risk of fraud based on a weighted combination of two different types of conventional fraud risk calculations (archetype-related and frequency-related) – does not change or improve how the *computer* functions even if

[2] We note that claim 1 does recite a "card-not-present (CNP) online transaction conducted over a communications network." Appeal Br. 22 (Claim 1). However, unlike in *Ancora Technologies* where the claimed method improves computer *functionality*, the above limitation in claim 1 merely "link the use of a judicial exception to a particular technological environment or field of use" (i.e., online transactions). Without more, such general linkage does not suffice to integrate the abstract idea into a practical application or to render the claim patent eligible. 84 Fed. Reg. 55.

improves fraud detection in a transaction conducted over a communications network.

Appellant further contends that, in order to provide the feedback relating to whether a transaction is fraudulent, "the transaction data received by the merchant transaction computer may be correlated with outside data such as a GPS device or other behavioral (e.g., frequency) data" and that, "[c]learly, this corresponds to transformation of information or data from one state of being to another." Appeal Br. 14–15.

We are not persuaded. Appellant appears to be arguing that claim 1 is patent-eligible because it meets the machine or transformation test. However, the "transformation of information or data" Appellant cites constitutes "mere manipulation or reorganization of data," which the Federal Circuit has explained does not satisfy the transformation prong. *CyberSource*, 654 F.3d at 1375.

Appellant argues that the limitations in claim 1 in addition to the alleged abstract idea are not well-known, routine, or conventional in the field. Appeal Br. 16–19. Appellant argues that, like the claims in *Bascom Global Internet Services, Inc. v. AT&T Mobility LLC*, 827 F.3d 1341 (Fed. Cir. 2016), claim 1 as a whole "includes an inventive concept that can be found in the non-conventional and non-generic arrangement of known, conventional pieces." *Id.* at 18; Reply Br. 14. Appellant similarly argues that, like the claims in *Amdocs (Israel) Limited v. Openet Telecom, Inc.*, 841 F.3d 1288 (Fed. Cir. 2016), claim 1 "describes the unconventional solution (enhanced fraud detection) of using the claimed technique to solve a technical problem of providing risk scores using temporal behavior maps." Appeal Br. 19. Appellant argues that "the claimed elements . . . , either individually or in an ordered combination, **are not found in the prior art**" and that, "for at least reason, Claim 1 cannot be said to contain only elements that are well-understood, routine, and conventional." *Id.* More particularly, Appellant contends that "[t]he Examiner agrees that **no one had previously provided archetype-related and frequency-related scores for fraud detection in CNP transactions**." Reply Br. 14; *see also* Reply Br. 18. Appellant contends that "[t]his inventive concept is not intuitive because '[f]or such CNP transactions business need to employ extra information on customers to detect fraud.'" *Id.* at 15.[3]

We are not persuaded. Once again, Appellant points only to the judicial exceptions (i.e., a particular method of detecting fraud through past transactions and the calculation of archetype-related and frequency-related fraud risk scores, which recite an abstract method of organizing human activity and mathematical concepts) as the claims' inventive concept. As we have discussed, however, under step 2 of the *Mayo*/Alice analysis the claim must recite *additional elements*, i.e., "claim features, limitations, and/or steps that are recited in the claim *beyond the identified judicial exception*," that provide "'significantly more' than the recited judicial exception." 84

[3] In the Appeal Brief, Appellant also points in particular to the concept of "adjusting fraud scores 'below the operation threshold, [wherein the] adjustment will not affect the fraud scoring model's performance at and above operation threshold." Appeal Br. 18. Appellant argues that this inventive concept is captured by the limitations of adjusting, in response to the detecting of a request or independent to the detecting, "the fraud scores for at least some of the plurality of transactions" in the high-score or the low-score bands, respectively. *Id.* These limitations, however, are not found in claim 1. Thus, this argument is inapposite.

Fed. Reg. at 55 n. 24 (defining "additional elements"), 56 (emphasis added); *see also Alice*, 573 U.S. at 217–218.

For similar reasons, *Bascom* and *Amdocs* are not analogous as Appellant argues. In *Bascom*, the Court found the claim to be directed to an abstract idea, i.e., filtering content. 827 F.3d at 1348. Nevertheless, the Court found that the claim is patent eligible because it discloses an inventive concept wherein a filtering tool is installed "at a specific location, remote from the end-users, with customizable filtering features specific to each end user." *Id.* at 1349. The claim in *Bascom* thus differs from instant claim 1, which does not describe any non-generic arrangement of the recited generic computer components. *See id.* at 1350 (explaining that "[a] claim[ ] would not contain an inventive concept" if it "merely recite [an] abstract idea . . . along with the requirement to perform it on the Internet, or to perform it on a set of generic components."

Likewise, in *Amdocs* the Court found that the claim contained a sufficient "inventive concept," because it read the claim limitation of "enhanc[ing] the first network accounting record" as being "dependent upon the invention's distributed architecture" and thus construed it as meaning "to apply a number of field enhancement in a distributed fashion," wherein distributed means that "the network usage records are processed close to their sources before being transmitted to a centralized manager." *Id.* at 1300 (internal quotation marks omitted). The *Amdocs* court further pointed out that, "[a]s explained by the patent, this distributed enhancement was a critical advancement over the prior art." *Id.* In light of the construction of the term "enhance," the court found that

> this claim entails an unconventional technological solution (enhancing data in a distributed fashion) to a technological problem (massive record flows which previously required massive databases). The solution requires arguably generic components, including network devices and "gatherers" which "gather" information. However, the claim's enhancing limitation necessarily requires that these generic components operate in an unconventional manner to achieve an improvement in computer functionality.

Id. at 1300–1301.

Like the claim in *Bascom* and unlike instant claim 1, therefore, the claim in *Amdocs* requires arguably generic computer components to be arranged and/or to operate in an unconventional (i.e., distributed) manner. In contrast, the only "inventive concept" Appellant has pointed to with respect to claim 1 is in the recited abstract concepts themselves.

Finally, Appellant contends that, as with the claims in *McRO,* claim 1 is "far from preempting all approaches of fraud detection in CNP transactions" and that "[t]he specific way of achieving a desired outcome or end result in claim 1 does not pre-empt or 'tie up' any abstract idea." Reply Br. 16.

We are not persuaded. "While preemption may signal patent ineligible subject matter, the absence of complete preemption does not demonstrate patent eligibility." *Ariosa Diagnostics, Inc. v. Sequenom, Inc.*, 788 F.3d 1371, 1379 (Fed. Cir. 2015). This is particularly the case where, as in this case, the claim recites only abstract ideas, generic computer components, and a limitation that merely "link the use of a judicial exception to a particular technological environment or field of use" (i.e., "a card-not-present (CNP) online transaction conducted over a communications network"). *See id.* ("Where a patent's claims are deemed only to disclose patent ineligible subject matter under the *Mayo* framework . . . , preemption concerns are fully addressed and made moot.").

Accordingly, we affirm the Examiner's rejection of claim 1 as being directed to a judicial exception to patent eligible subject matter, without significantly more. Claims 2–18, which are not separately argued, fall with claim 1.

CONCLUSION

In summary:

Claims Rejected	**35 U.S.C. §**	**Reference(s)/Basis**	**Affirmed**	**Reversed**
1–18	101	Eligibility	1–18	

TIME PERIOD FOR RESPONSE

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