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.
11/958,130	12/17/2007	Frank Ozment	15548.0143	1565

27890 7590 01/29/2020

STEPTOE & JOHNSON LLP
1330 CONNECTICUT AVENUE, N.W.
WASHINGTON, DC 20036

EXAMINER
GREGG, MARY M

ART UNIT	PAPER NUMBER
3697	

NOTIFICATION DATE	DELIVERY MODE
01/29/2020	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):

hfox@steptoe.com
ipdocketing@steptoe.com
lfielding@steptoe.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte FRANK OZMENT, CLAY DANIEL, and DEWAYNE JONES

Appeal 2018-004474
Application 11/958,130
Technology Center 3600

Before CYNTHIA L. MURPHY, KENNETH G. SCHOPFER, and TARA L. HUTCHINGS, *Administrative Patent Judges*.

MURPHY, *Administrative Patent Judge*.

DECISION ON APPEAL

The Appellant[1] appeals from the Examiner's rejection of claims 1–3, 5, 8–13, 15–19, 21, 24–29, 31–34, and 36 under 35 U.S.C. § 101.

We AFFIRM.[2]

---

[1] The Appellant is the "applicant" (e.g., "the inventor or all of the joint inventors") as defined in 37 C.F.R. § 1.42. "The real party in interest is Regions Financial Corporation." (Appeal Br. 3.)

[2] We have jurisdiction over this appeal under 35 U.S.C. § 134 and 35 U.S.C. § 6(b).

BACKGROUND

The Appellant provides a method for "controlling financial transactions." (Spec. 1, l. 15.) More specifically, the Appellant's method can control a credit-card transaction involving a "card," a "financial institution," and a "merchant." (Spec. 10, ll. 10–18.)

In the administrative stage of a credit-card transaction, administrative steps must be taken to form the financial framework for the transaction. For example, an account must be provided to fund purchases made with the credit card, and, at some point, the credit card must be issued to a user so that he/she can make a purchase therewith. (*See* Spec. 1, ll. 21–22; *see also* Reed[3] ¶ 34.) Also during this administrative stage, information to "verify the identity of the user" of the credit card must be established in order to "screen against fraudulent transactions" (Spec. 8, ll. 4–5; *see also* Golan[4] ¶¶ 3, 24); and purchase criteria must be established if it is desired to restrict credit-card purchases to certain items, certain merchants, and/or certain spending limits (*see* Spec. 3, ll. 21–23; *see also* Reed ¶¶ 3, 4, 16).

The Appellant uses the term "security parameters" to describe the user-authenticating and purchase-criteria information established during the administrative stage of a credit-card transaction. (*See, e.g.*, Spec. 8, ll. 4–9.) Thus, a security parameter for user-authenticating purposes can be, for example, a "card verification value code," and a security parameter for purchase-criteria purposes can be, for example, a "class[] of goods," a "merchant category code," and/or a "monetary value" (Spec. 8, ll. 7–9.) And, because these security parameters will come into play when the credit

[3] US 2006/0113376 A1, published June 1, 2006.

[4] US 2005/0097320 A1, published May 5, 2005.

card is used for a purchase, these security parameters can be "carr[ied" by, "encoded" on, and/or "stored" in the credit card. (Spec. 1, l. 17; 8, ll. 8–9; 10, l. 23.)

A credit-card transaction is initiated when a user "present[s] his or her card to a merchant" to make a purchase, and the merchant "run[s] the card through [its] terminal enabling the terminal to read the information on the card." (Spec. 10, ll. 18–19; *see also* Reed ¶ 43.) As indicated above, the security parameters are information carried by the credit card, and, therefore, the security parameters are read by the merchant's terminal.

"In a typical credit card transaction," the merchant "verifies" that "the bank that issued the credit card will pay the merchant the transaction amount." (Nelson[5] ¶ 2.) During this merchant-verification stage of a credit-card transaction, the merchant submits "an 'authorization request' to a processor responsible for authorizing transactions involving the credit card." (Nelson ¶ 2.) Put another way, the merchant transmits (via its terminal) a "transaction request" to the financial institution. (Spec. 1, l. 23.)

The transaction request transmitted to the financial institution includes the information read from the credit card, and thus includes the security parameters. (*See* Spec. 10, ll. 19–21.) The transaction request will also include "transaction parameter[s]" which are "generate[d]" by the merchant's terminal. (Spec. 8, ll. 12–13.) These merchant-generated transaction parameters correspond to the particulars of the proposed purchase, such as the merchant's name, the type of goods presented for purchase, and the price of these goods. (*See* Spec. 1, ll. 23–24; *see also* Nelson ¶ 4.)

[5] US 2005/0205662 A1, published September 22, 2005.

When the financial institution receives the transaction request from the merchant's terminal, it vets the transaction request to determine whether the proposed purchase is properly payable by the credit card. (*See, e.g.*, Spec. 8, ll. 4–9; *see also* Nelson ¶ 2.) In this vetting stage of a credit-card transaction, the financial institution can use the security parameter(s) to screen for fraudulent activity. (*See* Spec. 8, ll. 4–5.) For example, "[w]hen transactions contain indicia outside of the user security parameters," the financial institution "may block the transaction." (Spec. 10, ll. 6–8.)

Also during this vetting stage of the credit-card transaction, account control information (i.e., purchase-criteria information) is "compared to the transaction information" to see if the transaction "compl[ies] with all of the relevant account control information." (Nelson ¶ 4.) In other words, the financial institution compares the security parameter(s) to the transaction parameter(s) to see "[i]f a match is found." (Spec. 8, ll. 14–15.) If this comparison is "favorable," the financial institution notifies the merchant and the cardholder (e.g., by sending "an approval code") that the transaction can be completed. (Spec. 11, ll. 1–4.) If this comparison is "unfavorable," they are notified that the transaction should be "declined." (Spec. 11, l. 4.)

The Appellant describes its method in the context of a "disaster relief program" in which the credit card is issued to a "disaster victim." (Spec. 2, ll. 3–4.) In this context, the account allocated during the administrative stage is funded by a variety of sources, namely parties "willing to participate in [the] disaster relief program." (Spec. 3, ll. 6–9.) Also in this context, the purchase criteria set during the administrative stage is aligned with the objectives of the disaster relief program. (*See* Reed ¶ 4.) For example, the purchase criteria (and thus the security parameters) could correspond to

essential goods (e.g., home repair supplies and groceries), daily spending limits for these respective goods (e.g., $1000 for home repair supplies and $100 for groceries), and/or pre-approved merchants. (*See*, *e.g.*, Spec. 8, ll. 7–13.)

Thus, the Appellant's method comprises steps performed during the administrative, merchant-verification, and vetting stages of a typical credit-card transaction, with the administrative details of this transaction correlating with the financial characteristics of a disaster relief program.

ILLUSTRATIVE CLAIM

(with paragraphing revised and bracketed text added)

1. A computer-based method for controlling financial transactions, comprising:

[(a)] providing an allocated account by a financial institution wherein funds are allocated to the account by a plurality of sources,

[(b)] establishing a first security parameter by the financial institution to debit the allocated account,

[(c)] establishing a second security parameter by the financial institution to debit the allocated account,

wherein the security parameter is merchant category code, a card verification value code, a geographic location, a monetary value range, a transaction mode, an account access parameter, a class of goods, a daily upper limit for a maximum debit of funds, or a class of services;

wherein the plurality of sources provides an initial amount of funds to a user, through a financial institution,

wherein the first security parameter is designed to determine whether to authorize a transaction based on a type of good or service subject to the financial transaction,

wherein the sources are pooled sources and are not owned by the user and an agreement is secured from a

merchant regarding a geographic location, a monetary value range, a transaction mode, an account access parameter, a class of goods, a daily upper limit for a maximum debit of funds, or a class of services, before establishing a security parameter;

[(d)] issuing the transaction card to the user, the transaction card carrying data identifying the security parameters, wherein the security parameters are stored in the card;

[(e)] receiving a transaction request from a terminal,

[(f)] providing a server to transmit the request over a communications line wherein the server is configured to download an application to perform an analysis of the first and second security parameters to detect fraud,

[(g)] the transaction request transmitted along the communications line to the financial institution, the transaction request characterized by a transaction parameter;

[(h)] comparing the transaction parameter to the first security parameter to evaluate the transaction request wherein the transaction request is evaluated by a processor based on the type of good or service subject to the financial transaction;

[(i)] determining, based on the evaluated transaction parameters, whether to process the transaction request for a transaction by a processor,

wherein the transaction comprises a first balance and a second balance, and

wherein the first security parameter is applied toward the first balance, the second security parameter is applied toward the second balance;

[(j)] adjusting the security parameters by the financial institution if fraud is suspect for a predetermined period of time;

[(k)] providing notice of whether the request has been granted or denied to a user at the terminal by the financial institution; and

[(l)] displaying the notice on a client device.

REJECTION[6]

The Examiner rejects claims 1–3, 5, 8–13, 15–19, 21, 24–29, 31–34, and 36 under 35 U.S.C. § 101 as directed to a judicial exception (i.e., an "abstract idea") without significantly more. (Final Action 3.)

JUDICIAL EXCEPTIONS

The Patent Act defines subject matter eligible for patent protection as "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof." (35 U.S.C. § 101.) Yet the Supreme Court has "long held" that this provision contains an important implicit exception: "[l]aws of nature, natural phenomena, and abstract ideas are not patentable." (*Ass'n for Molecular Pathology v. Myriad Genetics, Inc.*, 569 U.S. 576, 589 (2013).) These three concerns are "judicially created exceptions to § 101," or more concisely, "judicial exceptions." (*McRO, Inc. v. Bandai Namco Games Am. Inc.*, 837 F.3d 1299, 1311 (Fed. Cir. 2016).) Thus, an abstract idea is a judicial exception to something (e.g., a method) that would otherwise be considered statutory subject matter.

THE *ALICE* TEST

In *Alice Corp. v. CLS Bank Int'l*, 573 U.S. 208 (2014), the Supreme Court provided a two-step test to detect when an attempt is being made to patent an abstract idea in isolation. (*Id.* at 217–18.) In *Alice* step one, a determination is made as to whether the claim at issue is "directed to" an abstract idea. (*Id.* at 218.) When doing *Alice* step one, attention can be

[6] The Examiner's rejections under 35 U.S.C. § 103 (*see* Final Action 65–138) have been withdrawn (*see* Answer 3–4).

given to whether an abstract idea recited in the claim has been integrated into a practical application. (*See id.* at 217.)

If the claim at issue is "directed to" an abstract idea, *Alice* step two must be performed. (*Alice*, 573 U.S. at 217–18.) In the second step of the *Alice* test, a determination is made as to whether "additional elements" in the claim, both individually and as an ordered combination, contribute "significantly more" than the abstract idea. (*Id.*) When doing *Alice* step two, attention is given to whether additional elements, and any ordered combination thereof, are "well-understood," "routine," or "conventional." (*Id.* at 225.)

2019 § 101 GUIDANCE

The 2019 Revised Patent Subject Matter Eligibility Guidance ("2019 § 101 Guidance") provides us with specific steps for discerning whether a claim passes the *Alice* test for patent eligibility. (*See* Federal Register Vol. 84, No. 4, 50–57.) These steps are "[i]n accordance with judicial precedent," and consist of a two-pronged Step 2A and a Step 2B. (*Id.* at 52.)

ANALYSIS

Independent claim 1 sets forth "[a] computer-based method for controlling financial transactions" comprising steps (a)–(l). (Appeal Br., Claims App.) The Examiner determines that independent claim 1 is directed to an abstract idea (e.g., a fundamental economic practice); and the Examiner determines that additional elements in the claim do not amount to significantly more than this abstract idea. (*See* Final Action 4–5.) More succinctly, the Examiner concludes that independent claim 1 does not pass the *Alice* test for patent eligibility.

Prong One of Step 2A

Per the 2019 § 101 Guidance, we begin our analysis with the first prong of Step 2A (Prong One), where we determine whether the claim at issue "recites" an abstract idea. (2019 § 101 Guidance, Federal Register Vol. 84, No. 4, 54.) The Guidance "extracts and synthesizes key concepts identified by the courts as abstract ideas," and these concepts include "[c]ertain methods of organizing human activity," particularly, "fundamental economic principles or practices," and, even more particularly, commercial "interactions." (*Id.* at 52.) Thus, a claim reciting a financial transaction involving a credit card (i.e., a credit-card transaction) recites an abstract idea.[7]

Step (a) recites "providing an allocated account by [the] financial institution," step (b) recites "establishing a first security parameter by the financial institution to debit the allocated account," step (c) recites "establishing a second security parameter by the financial institution to debit the allocated account," and step (d) recites "issuing the transaction card to the user." (Appeal Br., Claims App.)[8]

---

[7] In *Inventor Holdings, LLC v. Bed Bath & Beyond, Inc.*, 876 F.3d 1372 (Fed. Cir. 2017), a claim reciting a method for paying for a remote order (e.g., with a credit card) at a merchant's terminal was held to recite an abstract idea (*see id.* at 1378); in *Smart Systems Innovations, LLC v. Chicago Transit Authority*, 873 F.3d 1364 (Fed. Cir. 2017), a claim reciting the use of a bankcard to enter a mass transit system (i.e., a financial transaction equivalent to purchasing a fare card) was held to recite an abstract idea (*see id.* at 1372); and in *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366 (Fed. Cir. 2011), a claim reciting a method for verifying the validity of a credit-card transaction for Internet purchases was held to recite an abstract idea (*see id.* at 1371).

[8] The issued card "carr[ies] data identifying the security parameters, wherein the security parameters are stored in the card." (*Id.*)

Thus, steps (a)–(d) set forth administrative steps performed during the administrative stage of a typical credit-card transaction.

Step (e) recites "receiving a transaction request from a terminal," and step (g) recites that "the transaction request [is] transmitted along [a] communication line to the financial institution." (Appeal Br., Claims App.) This is just another way of saying that, when a credit card is presented to a merchant for a proposed purchase, the merchant transmits (via its terminal) a transaction request to the financial institution for verification that this purchase is properly payable by the credit card. And this transaction request will include (i.e., will be "characterized by") transaction parameters particularizing the proposed purchase. (*Id.*)

Thus, steps (e) and (g) set forth request-transmitting steps performed during the merchant-verification stage of a typical credit-card transaction.

Step (f) recites the performance of "an analysis of the first and second security parameters to detect fraud," step (j) recites "adjusting the security parameters by the financial institution if fraud is suspect for a predetermined period of time,"[9] step (h) recites "comparing the transaction parameter to the first security parameter to evaluate the transaction request," step (i) recites "determining, based on the evaluated transaction parameters, whether to process the transaction request," step (k) recites "providing notice of whether the request has been granted or denied to a user at the terminal by the financial institution," and step (l) recites "displaying the notice on a client device." (Appeal Br., Claims App.)

[9] Thus, a security parameter could be, for example, "a card verification value code" that would, of course, need to be changed by the financial institution if it suspected fraudulent activity. (Appeal Br., Claims App.)

Thus, steps (f) and (i)–(l) set forth analyzing, comparing, determining, and informing steps performed during the vetting stage of a typical credit-card transaction.

Independent claim 1 also recites administrative details that might differ somewhat from those of a typical credit-card transaction, in that they are characteristic to a credit-card transaction in the context of the disaster-relief program. Specifically, the account allocated in step (a) would be funded by contributions from multiple parties (i.e., "a plurality of sources") willing to participate in the disaster relief program. (Appeal Br., Claims App.) The contributed funds would be "pooled," would be "not owned" by the disaster victims, and would, of course, include "an initial amount of funds." (*Id.*)

Also, the purchase criteria (i.e., security parameters) established in steps (b) and (c) understandably align with objectives of the disaster-relief program. For example, the purchase criteria could limit credit card purchases to disaster-relief goods (e.g., home repair supplies and groceries) and set daily spending limits for these goods (e.g., $1000 for home repair supplies and $100 for groceries). If so, security parameters could be "a class of goods," "a daily upper limit," and/or "designed to determine whether to authorize a transaction based on a type of good or service subject to the financial transaction." (Appeal Br., Claims App.)[10]

Additionally or alternatively, a disaster relief program may want credit card purchases to be made only from a pre-approved merchant that it

[10] And when "the transaction comprises a first balance and a second balance," a first security parameter would be "applied toward the first balance," and a second security parameter would be "applied toward the second balance." (Appeal Br., Claims App.)

considers best suited to serve disaster victims. If so, "before establishing a security parameter" corresponding to this pre-approved merchant, "an agreement is secured from [the] merchant." (Appeal Br., Claims App)[11]

Consequently, independent claim 1 recites steps performed during the administrative, merchant-verification, and vetting stages of a typical credit-card transaction. Inasmuch as administrative details recited in independent claim 1 confine this credit-card transaction to a particular context (i.e., a disaster-relief program), it is still a credit-card transaction.[12] A credit-card transaction is a fundamental economic practice (e.g., a commercial interaction), which is a certain method of organizing human activity that constitutes an abstract idea. (*See* 2019 § 101 Guidance, Federal Register Vol. 84, No. 4, 52.)

Thus, independent claim 1 recites an abstract idea under Prong One of Step 2A of the 2019 § 101 Guidance, and so we proceed to the second prong (Prong Two) of Step 2A.

Prong Two of Step 2A

In Prong Two, we determine "whether the claim as a whole integrates the recited judicial exception into a practical application of the exception."

---

[11] This agreement could be in regards to "a geographic location, a monetary value range, a transaction mode, an account access parameter, a class of goods, a daily upper limit for a maximum debit of funds, or a class of services." (Appeal Br., Claims App.)

[12] Comparably, a credit-card transaction in the context of a mass-transit system is still a credit-card transaction (*see Chicago Transit Authority*, 837 F.3d at 1372); and a credit-card transaction in the context of Internet purchases is still a credit-card transaction (*see Cybersource*, 654 F.3d at 1370).

(2019 § 101 Guidance, Federal Register Vol. 84, No. 4, 54.) In doing this determination, we identify "whether there are any additional elements recited in the claim beyond the judicial exception(s)," and we evaluate "those additional elements individually and in combination to determine whether they integrate the exception into a practical application." (*Id.* at 54–55.)

Independent claim 1 recites a "[software] application," a "server," and "processor[s]." (Appeal Br., Claims App.) These computer components are additional elements in the claim beyond the abstract idea of a credit-card transaction. Thus, we must evaluate whether these computer components, individually, integrate the recited credit-card transaction into a practical application.

When an additional element in a claim is a "computer," the relevant question is not whether the claim requires the computer to accomplish a recited function. (*Alice*, 573 U.S. at 223.) Rather, "the relevant question" is whether the claim does more than simply "instruct the practitioner to implement the abstract idea" on a computer. (*Id.* at 225.) The mere recitation of a computer in the claim, and/or words simply saying "apply" the abstract idea "with a computer," will not transform the "abstract idea into a patent-eligible invention." (*Id.* at 223.) In short, the sheer introduction of a computer into the claim is not enough to "impart patent eligibility." (*Id.*)

Independent claim 1 recites that the software application is "to perform an analysis of the first and second security parameters to detect fraud." (Appeal Br., Claims App.) This analysis amounts to the screening of credit-card information for fraudulent activity, which is a vetting step in a credit-card transaction. And, per the Specification, this analysis can be as

uncomplicated as the financial institution looking for "indicia outside of the user security parameters." (Spec. 10, ll. 6–8.) Thus, claim 1 simply instructs a practitioner to use an undefined software application to implement this straightforward review of the credit card's indicia.

Independent claim 1 recites "providing" the server "to transmit the [transaction] request over a communications line." (Appeal Br., Claims App.) As discussed above, the transmission of the transaction request from the merchant to the financial institution is a step in the merchant-verification stage of a credit-card transaction. Thus, claim 1 simply instructs a practitioner to use a server to implement this merchant-verification step.

Independent claim 1 recites that the transaction request "is evaluated by a processor based on the type of good or service subject to the financial transaction." (Appeal Br., Claims App.) The evaluation of whether a proposed credit-card purchase meets the administrative criteria set for this credit card (i.e., only certain types of goods or services can be purchased) is part of the vetting stage of a credit-card transaction. Thus, claim 1 simply instructs the practitioner to use a processor to implement this vetting step.

Independent claim 1 recites determining "whether to process the transaction request for a transaction by a processor." (Appeal Br., Claims App.) This determination by a financial institution is also part of the vetting stage of a credit-card transaction. Thus, claim 1 simply instructs a practitioner to use another processor to implement another vetting step.

Consequently, none of the recited computer components, individually, integrate the abstract idea of a credit-card transaction into a practical application. However, the 2019 § 101 Guidance requires us to look at independent claim 1 as a whole in our evaluation of whether the abstract

idea has been integrated into a practical application. (*See* 2019 § 101 Guidance, Federal Register Vol. 84, No. 4, 54.) Even when additional elements are not enough on their own to meaningfully limit an exception, the claimed combination of these additional elements may still provide the practical application. (*See id.*)

Independent claim 1 recites that the server is "configured to download" the software application. (Appeal Br., Claims App.) Other than that, claim 1 requires no specific interaction between, and no specific arrangement of, the computer components. For example, there is no claimed relationship between the two processors; and there is no claimed relationship between the processor(s) and the server (and/or the software application downloaded thereon). As such, claim 1 does not set forth a combination of computer components capable of integrating the abstract idea into a practical application.

Thus, independent claim 1 as a whole, does not integrate the recited credit-card transaction into a practical application under Prong Two of Step 2A of the 2019 § 101 Guidance, and so we proceed to Step 2B.

Step 2B

In Step 2B, we evaluate whether the additional elements recited in the claim, individually or in combination, amount to "significantly more" than the abstract idea itself. (2019 § 101 Guidance, Federal Register Vol. 84, No. 4, 56.) If the additional elements consist of a conventional arrangement of well-understood, routine, conventional computer components, they will not amount to significantly more, and the claim fails the *Alice* test for patent eligibility. (*Id.*) Here, the Specification describes the software/hardware

components, and their arrangement, as generic and conventional. (*See* Spec. 11, ll. 14–23; Fig. 1.)[13]

Thus, independent claim 1 fails the *Alice* test for patent eligibility, and does not pass muster under 35 U.S.C. § 101.

The Appellant's Arguments

The Appellant argues that independent claim 1 "overcome[s] a problem in an inventive way by taking advantage of the technical capabilities of servers and computer technology in the specific claimed order and combination." (Appeal Br. 13.) However, the problem addressed by the Appellant is controlling credit-card transactions in the context of a disaster relief program. And this problem is solved by administratively aligning purchase criteria for a credit card (issued to a disaster victim) with the objectives of the disaster relief program. This solution is administrative in nature, and, in any event, unrelated to the technical capabilities of the computer components recited in the claim.[14] We disagree, therefore, with

[13] Insofar as the "terminal," the "communication line," and/or the "client device" also constitute additional elements, they are simply used as tools when performing steps that occur during a typical credit-card-transaction; they are not arranged in any ordered combination; and they are described (if at all) as conventional in the Specification. (*See e.g.*, Spec. 10, ll. 17–23; 11, 2–4; Fig. 1.)

[14] Prior art of record shows that the concept of a credit-card transaction in the context of a disaster relief program is not new. (*See* Reed ¶ 4.) But even if this concept was new (and/or if the claimed method includes novel administrative steps for carrying it out), this merely means that the Appellant is claiming a "new" abstract idea. A new abstract idea, even if it is a "brilliant" abstract idea, "does not by itself satisfy the § 101 inquiry." (*Ass'n for Molecular Pathology*, 569 U.S. at 591.)

the Appellant's assertion that independent claim 1 is directed to a "specific" method "in the field of data processing and computer networks." (*Id.*)

The Appellant argues that "**even if** elements of [a] claim are known or generic, the specific combination or order may provide an inventive concept." (Appeal Br. 13.) We do not disagree.[15] The trouble with this argument is that, here, independent claim 1 does not require any specific combination of the recited computer components. As discussed above, there is no claimed relationship between the software application, the server, and/or the processors.

The Appellant argues that "[a] computer is integral" to the method set forth in independent claim 1. (Appeal Br. 12.) In this regard, the Appellant puts emphasis on step (g), which requires "adjusting the security parameters by the financial institution if fraud is suspect for a predetermined period of time." (*Id.*, Claims App.) According to the Appellant, "[t]his claimed feature cannot exist but for a computer programmed to flag or adjust security parameters as claimed, e.g.[,] in a dynamic fashion." (*Id.*) However, step (g) does not require this adjustment to be performed by a computer, and/or in a dynamic fashion. Step (g) simply requires the financial institution to update its security strategy (i.e., adjust security parameters) when fraud is suspected, which would seem to be the logical administrative response to such a suspicion.

---

[15] Indeed, in *Bascom Global Internet Services Inc. v. AT&T Mobility LLC*, 827 F.3d 1341 (Fed. Cir. 2016), the Federal Circuit expressly stated that it is sometimes possible for "an inventive concept" to reside in "the non-conventional and non-generic arrangement of known, conventional pieces," such as "a set of generic computer components." (*Id.* at 1350.)

Thus, after careful consideration of the Appellant's arguments, we are not convinced that the Examiner wrongly concludes that independent claim 1 recites a judicial exception without significantly more.

Summary

We agree with the Examiner that independent claim 1 fails the *Alice* test of patent eligibility, and, therefore, does not pass muster under 35 U.S.C. § 101. The claims on appeal are argued as group (*see* Appeal Br. 11–14), and so claims 2, 3, 5, 8–13, 15–19, 21, 24–29, 31–34, and 36 fall with independent claim 1.[16]

CONCLUSION

Claims Rejected	35 U.S.C. §	Reference(s)/Basis	Affirmed	Reversed
1–3, 5, 8–13, 15–19, 21, 24–29, 31–34, 36	101	Eligibility	1–3, 5, 8–13, 15–19, 21, 24–29, 31–34, 36	

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

AFFIRMED

[16] "When multiple claims subject to the same ground of rejection are argued as a group or subgroup by appellant, the Board may select a single claim from the group or subgroup and may decide the appeal as to the ground of rejection with respect to the group or subgroup on the basis of the selected claim alone." (37 C.F.R. § 41.37(c) (1)(iv).)