



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.
13/444,263	04/11/2012	Michael Henry FIORE	0076412-000048	4509
21839	7590	11/12/2019	EXAMINER	
BUCHANAN, INGERSOLL & ROONEY PC POST OFFICE BOX 1404 ALEXANDRIA, VA 22313-1404			QAYYUM, ZESHAN	
			ART UNIT	PAPER NUMBER
			3685	
			NOTIFICATION DATE	DELIVERY MODE
			11/12/2019	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):

ADIPDOC1@BIPC.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte MICHAEL HENRY FIORE and MAX CHION

Appeal 2018-000670
Application 13/444,263
Technology Center 3600

Before MAHSHID D. SAADAT, BETH Z. SHAW, and
NORMAN H. BEAMER, *Administrative Patent Judges*.

BEAMER, *Administrative Patent Judge*

DECISION ON APPEAL

Appellant¹ appeals under 35 U.S.C. § 134(a) from the Examiner's Final Rejection of claims 1–3, 5–19, 21, and 23–35. Claims 4, 20, and 22 are cancelled. We have jurisdiction over the pending rejected claims 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 MasterCard International Incorporated. (Appeal Br. 2.)

THE INVENTION

Appellant's disclosed and claimed invention is directed to authentication of payment transactions using geographical location information provided by a mobile device to determine that the mobile device has entered a premises of a merchant. (Abstract.)

Independent claim 1, reproduced below, is illustrative of the subject matter on appeal:

1. A method for two-stage authentication of a user of a mobile device for a payment account number transaction, the method comprising:

storing, in a storage device of a managing computer system, at least one payment account number of a user in association with a mobile device of the user;

identifying, by a processing device of the managing computer system, a location of the mobile device at a particular merchant's physical location;

providing, by the processing device, first authentication data of the user of the at least one payment account number for payment transactions with the merchant upon the mobile device entering a premises of the merchant, wherein the user is authenticated for future transactions at the merchant based upon the provided first authentication data;

storing, in the storage device, an indication that the user is authenticated based upon the provided first authentication data; and

receiving, by the processing device, second authentication data, said second authentication data received from the user as part of a payment transaction against the at least one payment account number associated with said mobile device, wherein the payment transactions is initiated at said merchant,

wherein the user is authenticated based upon the provided first authentication data prior to the initiation of the payment transaction at said merchant.

REJECTIONS

The Examiner rejected claims 1–3, 5–19, 21, and 23–35 under 35 U.S.C. § 101 as being directed to non-statutory subject matter. (Final Act. 4–7.)

The Examiner rejected claims 1–3, 5–19, 21, and 23–35 under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. (Final Act. 7–9.)

The Examiner rejected claims 1–3, 5–19, 21, and 23–35 under 35 U.S.C. § 112, second paragraph, as indefinite. (Final Act. 9–10.)

The Examiner rejected claims 1–3, 5–8, 11–19, 21, and 23–35 under 35 U.S.C. § 103, as being unpatentable over Zambelli (US 2013/0198076 A1, published August 1, 2013) and Fourez (US 2011/0047075 A1, published February 24, 2011). (Final Act. 11–20.)

The Examiner rejected claims 9–10 under 35 U.S.C. § 103, as being unpatentable over Zambelli, Fourez, and Patel (US 2010/0332339 A1, published December 30, 2010). (Final Act. 20–22.)

ISSUES ON APPEAL

Appellant’s arguments present the following issues:²

Issue One: Whether the Examiner erred in concluding claims 1–3, 5–19, 21, and 23–35 are directed to non-statutory subject matter. (Appeal Br. 6–15.)

² Rather than reiterate the arguments of Appellant and the positions of the Examiner, we refer to the Appeal Brief (filed Mar. 27, 2017; suppl. May 24,

Issue Two: Whether the Examiner erred in finding claims 1–3, 5–19, 21, and 23–35 fail to comply with the written description requirement. (Appeal Br. 15–18.)

Issue Three: Whether the Examiner erred in concluding claims 1–3, 5–19, 21, and 23–35 are indefinite. (Appeal Br. 18–19.)

Issue Four: Whether the combination of Zambelli and Fourez teach or suggest the independent claim 1 limitation, “providing, by the processing device, first authentication data of the user of the at least one payment account number for payment transactions with the merchant upon the mobile device entering a premises of the merchant,” and the commensurate limitations of independent claims 19 and 34. (Appeal Br. 19–22.)

Issue Five: Whether the combination of Zambelli and Fourez teach or suggest the additional limitations of claims 3, 5–8, 11–18, 21, and 23–33, and 35, and whether the combination of Zambelli, Fourez, and Patel teach or suggest the additional limitations of claims 9 and 10. (Appeal Br. 22–23.)

ANALYSIS

Issue One

The Examiner concludes claims 1–3, 5–19, 21, and 23–35 are patent-ineligible under 35 U.S.C. § 101 because the claims are “directed to authenticating the user in order to initiate the payment transaction which is considered to be an abstract idea as such activity is considered both a fundamental economic practice and a method of organizing human activity.” (Final Act. 5.) The Examiner further concludes that there is nothing in the

2017); the Reply Brief (filed Oct. 23, 2017); the Final Office Action (mailed July 14, 2016); and the Examiner’s Answer (mailed Aug. 22, 2017) for the respective details.

claims that is significantly more than this abstract idea, but are “merely the combined and coordinated execution of generic computer functionalities which are well-understood, routine and conventional activities previously known to the industry.” (Final Act. 6.)

Appellant argues the Examiner unfairly overgeneralizes the claims, citing *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327 (Fed. Cir. 2016), *McRO, Inc. v. Bandai Namco Games Am. Inc.*, 837 F.3d 1299 (Fed. Cir. 2016), and *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245 (Fed. Cir. 2014), and arguing “the present claims should be accurately characterized as being directed to a technical process setting forth the steps of how to improve a particular type of authentication.” (Appeal Br. 6–10.)

Appellant further relies on *DDR Holdings* and *Bascom Glob. Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341 (Fed. Cir. 2016), and argue that the claims encompass “significantly more” than an abstract idea:

In a similar manner to the claims at issue in *DDR Holdings*, it is respectfully submitted that the appealed claims do not have a “real world” equivalent. That is, there is no “abstract business practice” to which Appellant's claims can be fairly analogized. Instead, Appellant's claims address a problem arising out of the existence of complex electronic payment networks and the susceptibility of such networks to fraudulent transactions.

* * *

Similar to the claims of *Bascom*, Appellant's claims harness technical features of certain technology (*e.g.*, the ability of mobile devices to transmit authentication data, etc.) to improve authentication processes in electronic payment transaction networks. The claims offer concrete technical solutions to technical problems existing in the fields of electronic transaction processing, identity protection in electronic processing, and information technology management and security.

(Final Act. 11–15.) For the reasons set forth below, we are not persuaded the Examiner erred.

An invention is patent-eligible if it claims a “new and useful process, machine, manufacture, or composition of matter.” 35 U.S. C. § 101. Here, independent claim 1 and its dependent claims relate to a method, independent claim 19 and its dependent claims relate to a system, and independent claim 34 relates to a non-transitory computer-readable recording medium — each a process, machine or manufacture. However, the Supreme Court has long held that “[l]aws of nature, natural phenomena, and abstract ideas are not patentable.” *Alice Corp. Pty. Ltd. v. CLS Bank Int’l*, 573 U.S. 208, 216 (2014) (quoting *Assoc. for Molecular Pathology v. Myriad Genetics, Inc.*, 569 U.S. 576, 598–99 (2013)). The “abstract ideas” category embodies the longstanding rule that an idea, by itself, is not patentable. *Alice*, 573 U.S. at 216–217.

In *Alice*, the Supreme Court sets forth an analytical “framework for distinguishing patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of those concepts.” *Id.* at 217. The first step in the analysis is to “determine whether the claims at issue are directed to one of those patent-ineligible concepts,” such as an abstract idea. *Id.* Concepts determined to be abstract ideas, and thus patent ineligible, include certain methods of organizing human activity such as fundamental economic practices (*Alice*, 573 U.S. at 219–20; *Bilski v. Kappos*, 561 U.S. 593, 611 (2010)); mathematical concepts (*Parker v. Flook*, 437 U.S. 584, 594–95 (1978)); and mental processes (*Gottschalk v. Benson*, 409 U.S. 63, 69 (1972)). Concepts determined to be patent eligible include physical and chemical processes, such as “molding rubber products”

(*Diamond v. Diehr*, 450 U.S. 175, 191 (1981)); “tanning, dyeing, making water-proof cloth, vulcanizing India rubber, smelting ores” (*id.* at 182 n.7 (quoting *Corning v. Burden*, 56 U.S. 252, 267–68 (1853))); and manufacturing flour (*Benson*, 409 U.S. at 69 (citing *Cochrane v. Deener*, 94 U.S. 780, 785 (1876))).

If the claims are directed to a patent-ineligible concept, the second step in the *Alice/Mayo* analysis is to consider the elements of the claims “individually and ‘as an ordered combination’” to determine whether there are additional elements that “‘transform the nature of the claim’ into a patent-eligible application.” 573 U.S. at 217 (quoting *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 79, 78 (2012)). In other words, the second step is to “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.’” 573 U.S. at 217–218 (quoting *Mayo*, 566 U.S. at 72–73.) A claim that recites an abstract idea must include additional features to ensure that the claim is more than a drafting effort designed to monopolize the abstract idea. 573 U.S. at 221. A transformation into a patent-eligible application requires more than simply stating the abstract idea while adding the words “apply it.” *Id.*

Further to the *Alice/Mayo* analytical framework, after the mailing of the Answer and the filing of the Briefs in this case, the USPTO published revised guidance on the application of Section 101. *See 2019 Revised Patent Subject Matter Eligibility Guidance*, 84 Fed. Reg. 50 (Jan. 7, 2019) (hereinafter “Revised Guidance”). Under the Revised Guidance, we first look to whether the claim recites:

(1) any judicial exceptions, including certain groupings of abstract ideas (i.e., mathematical concepts, certain methods of organizing human activity such as a fundamental economic practice, or mental processes); and

(2) additional elements that integrate the judicial exception into a practical application (*see* MPEP § 2106.05(a)–(c), (e)–(h)).

Only if a claim (1) recites a judicial exception and (2) does not integrate that exception into a practical application, does the Office then look to whether the claim:

(3) adds a specific limitation beyond the judicial exception that are not “well-understood, routine, conventional” in the field (*see* MPEP § 2106.05(d)); or

(4) simply appends well-understood, routine, conventional activities previously known to the industry, specified at a high level of generality, to the judicial exception.

See Revised Guidance.

In evaluating the claims at issue, we consider claim 1 as representative, consistent with how Appellant and the Examiner analyze the claims. *See* 37 C.F.R. § 41.37(c)(1)(iv)(2016). As stated in the preamble, claim 1 is focused on “two-stage authentication of a user of a mobile device for a payment account number transaction.” Omitting the portions of the claim invoking use of generic computer technology (which are discussed separately below), the remaining limitations of claim 1 elaborate on two-stage authentication of a transaction: (i) “storing . . . at least one payment account number of a user in association with a mobile device of the user”; (ii) “identifying . . . a location of the mobile device at a particular merchant's physical location”; (iii) “providing . . . first authentication data of the user of the at least one payment account number for payment transactions with the

merchant upon the mobile device entering a premises of the merchant, wherein the user is authenticated for future transactions at the merchant based upon the provided first authentication data”; (iv) “storing . . . an indication that the user is authenticated based upon the provided first authentication data”; (v) “receiving second authentication data, said second authentication data received from the user as part of a payment transaction against the at least one payment account number associated with said mobile device, wherein the payment transactions is initiated at said merchant”; and (vi) “wherein the user is authenticated based upon the provided first authentication data prior to the initiation of the payment transaction at said merchant.” (Suppl. Appeal Br. 3.)³

Apart from the use of generic technology (discussed further below), each of these limitations describes activities that could readily be performed by a payment account user (*e.g.*, using a credit card), a merchant, and a typical intermediary authentication service. In facilitating authentication of a payment transaction: the first limitation (i) provides for a user to associate a payment account with a mobile device; limitations (ii)–(iv) provide for the first stage of authentication based on the mobile device being located at the merchant location, and limitations (v)–(vi) provide for the second stage of the authorization of the payment transaction.

As stated in the Revised Guidance, commercial interactions are an example of organizing human activity, and in particular a fundamental

³ The Examiner appropriately paraphrased these elements: “storing in a storage device . . . ; identifying a location of the mobile device . . . ; providing first authentication data . . . ; storing . . . ; and receiving a second authentication data” (Final Act. 5.)

economic practice. (Revised Guidance, 84 Fed. Reg. at 52). The interaction between those involved in authenticating a payment transaction falls under this description. Analogous authority includes, *e.g.*, *Credit Acceptance v. Westlake Services*, 859 F.3d 1044, 1054 (Fed. Cir. 2015) (processing an application for financing a purchase); *Inventor Holdings, LLC v. Bed Bath & Beyond, Inc.*, 876 F.3d 1372, 1378–79 (Fed. Cir. 2017) (local processing of payments for remotely purchased goods); *buySAFE, Inc. v. Google, Inc.*, 765 F.3d 1350, 1355 (Fed. Cir. 2014) (creating a contractual relationship — a “transaction performance guaranty”); *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366 (Fed. Cir. 2011) (verifying the validity of a credit card transaction); *Dealertrack v. Huber*, 674 F.3d 1315, 1331 (Fed. Cir. 2012) (processing credit applications through a clearinghouse); *Smart Sys. Innovations, LLC v. Chicago Transit Auth.*, 873 F.3d 1364 (Fed. Cir. 2017) (regulating entry in a transit system using information from a bankcard, such as a credit card or debit card).

In sum, the subject matter of claim 1 is properly characterized as a fundamental economic practice, which is one of the certain methods of organizing human activity identified in the Revised Guidance. Therefore, we agree with the Examiner that the subject matter of claim 1 recites an abstract idea, as do the remaining claims.

Further pursuant to the Revised Guidance, we consider whether there are additional elements set forth in claim 1 that integrate the judicial exception into a practical application. Revised Guidance, 84 Fed. Reg. at 54–55. As indicated above, the abstract idea of claim 1 is carried out using generic computer technology to authenticate the payment transaction: a “managing computer system” including a “storage device” and a “processing

device.” (Suppl. Appeal Br. 3.) This is confirmed by statements in the Specification. (Ans. 6 (*citing* Spec. ¶¶ 33, 52); *see also* Spec. ¶ 38.)

None of these additional elements integrate the judicial exception into a practical application. The use of this computer technology may improve the fundamental economic practice of authenticating payment transactions, but nothing in the claims relate to an improvement in the functioning of a computer, or an improvement to other technology or technical field. Revised Guidance, 84 Fed. Reg. at 55.

Thus, the subject matter here is distinguished from that considered in such authorities as *BASCOM Global Internet Services, Inc. v. AT&T Mobility LLC*, 827 F.3d 1341 (Fed. Cir. 2016). There, the court held eligible claims directed to a technology-based solution to filter Internet content that overcame existing problems with other Internet filtering systems by making a known filtering solution—namely a “one-size-fits-all” filter at an Internet Service Provider (ISP)—more dynamic and efficient via individualized filtering at the ISP. *BASCOM*, 827 F.3d at 1351. Notably, this customizable filtering solution improved the computer system’s performance and, therefore, was patent-eligible. *See id.* But unlike the filtering system improvements in *BASCOM* that added significantly more to the abstract idea in that case, the claimed invention here uses generic computing components to implement an abstract idea, as noted previously.

Nor is this invention analogous to that which the court held eligible in *McRO, Inc. v. Bandai Namco Games America, Inc.*, 837 F.3d 1299 (Fed. Cir. 2016). There, the claimed process used a combined order of specific rules that rendered information in a specific format that was applied to create a sequence of synchronized, animated characters. *McRO*, 837 F.3d at 1315.

Notably, the recited process automatically animated characters using particular information and techniques—an improvement over manual three-dimensional animation techniques that was not directed to an abstract idea. *Id.* at 1316.

But unlike the claimed invention in *McRO* that improved how the physical display operated to produce better quality images, the claimed invention here merely uses generic computing components to store and process data. This generic computer implementation does not improve a display mechanism as was the case in *McRO*. See *SAP Am. v. InvestPic, LLC*, 898 F.3d 1161, 1167 (Fed. Cir. 2018) (distinguishing *McRO*).

Likewise, we disagree with Appellant that this a case involving eligible subject matter as in *DDR Holdings, LLC v. Hotels.Com, L.P.*, 773 F.3d 1245 (Fed. Cir. 2014). There, instead of a computer network operating in its normal, expected manner by sending a website visitor to a third-party website apparently connected with a clicked advertisement, the claimed invention in *DDR* generated and directed the visitor to a hybrid page that presented: (1) product information from the third party, and (2) the visual “look and feel” elements from the host website. *DDR*, 773 F.3d at 1258–59. Given this particular Internet-based solution, the court held that the claimed invention did not merely use the Internet to perform a business practice known from the pre-Internet world, but rather was necessarily rooted in computer technology to overcome a problem specifically arising in computer networks. *Id.* at 1257.

That is not the case here. As noted previously, Appellant’s claimed invention, in essence, relates to authentication of payment transactions. Appellant uses generic computer-based components to achieve that end. We

find the claimed invention on appeal is not necessarily rooted in computer technology in the sense contemplated by *DDR*, in which the claimed invention solved a challenge particular to the Internet. Although Appellant's invention uses various computer-based components as noted above, the claimed invention does not solve a challenge particular to the computing components used to implement this functionality.

Although the use of these computer-oriented techniques facilitate the authentication of payment transactions, “merely adding computer functionality to increase the speed or efficiency of the process does not confer patent eligibility on an otherwise abstract idea.” *Intellectual Ventures I LLC v. Capital One Bank (USA)*, 792 F.3d 1363, 1370 (Fed. Cir. 2015); *see also Credit Acceptance Corp. v. Westlake Services*, 859 F.3d 1044, 1057 (Fed. Cir. 1057). Otherwise, Appellant provides only conclusory, unpersuasive assertions that the subject matter provides any improvements to technology. (Appeal Br. 11–15.)

Nor does the subject matter of claim 1 contain additional elements that implement the judicial exception with a “particular machine,” because the claims do not specify any particular technology. *See* MPEP § 2106.05 (b). Further, the method does not transform matter; at best it transforms information. *See* MPEP § 2106.05(c). Nor does claim 1 have any other meaningful limitations (MPEP § 2106.05 (e)), or any of the other considerations set forth in the Revised Guidance regarding a determination of whether additional elements integrate the judicial exception into a practical application. *See* Revised Guidance, 84 Fed. Reg. at 55. Rather, the claim “merely includes instructions to implement an abstract idea on a computer, or merely uses a computer as a tool to perform an abstract idea.”

Id. Accordingly, we conclude that the subject matter of claim 1 (and the remaining pending claims) is directed to a fundamental economic practice, which is one of the certain methods of organizing human activity, and thus an abstract idea, and the additional elements recited therein do not integrate the abstract idea into a practical application.

Turning to the second step of the *Alice* inquiry, we do not agree with Appellant that additional elements of claim 1 add “significantly more” to the basic abstract idea encompassed by the claim sufficient to transform the claimed abstract idea into a patent-eligible application. *Alice*, 573 U.S. at 223 (“[T]he mere recitation of a generic computer cannot transform a patent-ineligible abstract idea into a patent-eligible invention.”). As discussed above, Appellant cites the improvements that “address a problem arising out of the existence of complex electronic payment networks and the susceptibility of such networks to fraudulent transactions.” (Appeal Br. 13.) However, other than using generic technology, these improvements are elaborations on the basic abstract idea itself. “It is clear from *Mayo* that the ‘inventive concept’ cannot be the abstract idea itself.” *Aatrix Software, Inc. v. Green Shades Software, Inc.*, 890 F.3d 1354, 1359 (Fed. Cir. 2018). Moreover, “[p]atent law does not protect claims to an ‘asserted advance in the realm of abstract ideas ... no matter how groundbreaking the advance.’” 890 F.3d at 1359 (Fed. Cir. 2018).

The record supports the Examiner’s finding that the additional elements — a processor and a storage device — are well-understood, routine, and conventional, specified at a high level of generality. (Ans. 6 (citing Spec. ¶¶ 33, 52); see also Spec. ¶ 38.) Revised Guidance, 84 Fed. Reg. at 56.

Accordingly, we sustain the Examiner's 35 U.S.C. § 101 rejection of claim 1. Appellant provides no arguments that would differentiate the remaining claims. Thus, the foregoing analysis of claim 1 is exemplary of that for claims 2, 3, 5–19, 21, 23–35. *See* 37 C.F.R. § 41.37(c)(1)(iv)(2016). Therefore, we also sustain the Examiner's 35 U.S.C. § 101 rejection of those claims.

Issue Two

The Examiner finds that the following limitations of independent claim 1 does not comply with the written description requirement:

providing, by the processing device, first authentication data of the user of the at least one payment account number for payment transactions with the merchant upon the mobile device entering a premises of the merchant; and

storing, in the storage device, an indication that the user is authenticated based upon the provided first authentication data.

(Final Act. 7–9.) The Examiner also finds that the limitation of claim 12, “revoking, by the processing device, the authentication based upon the first authentication data,” lacks written description support. (*Id.* at 9.)

Appellant argues these limitations are supported by Figures 4A and 4B, and accompanying description, which explain that when a mobile device is in proximity to a particular merchant, an indication of that fact is entered into an “authentication table,” which entry serves to pre-authenticate the transaction, and which entry is revoked when the mobile device is no longer at that location. (Appeal Br. 16–18; Spec. Figs. 4A, 4B, ¶¶ 39, 46–50, 54–55.) The “authentication data” manifests that a particular mobile device is at a particular location, which in turn is the basis for the claimed “indication”

stored in the storage device. We agree with Appellant, and accordingly do not sustain these written description rejections.

Issue Three

The Examiner concludes that the claim 1 limitation, “providing, by the processing device, first authentication data of the user of the at least one payment account number for payment transactions,” is indefinite, because “it is unclear whether the first authentication data is provided to the user or merchant.” (Final Act. 10.) As discussed above, in the context of the claim, the authentication data is “provid[ed]” by the processing device, and forms the basis for an “indication” stored in the storage device. Aside from serving as the basis for the claimed “indication,” the claim is agnostic as to any further disposition of the authentication data, and neither requires nor forbids the authentication data to be provided to the user or the merchant. (Appeal Br. 18.) Therefore, we do not sustain this indefiniteness rejection.

The Examiner further concludes that the claim 1 limitation, “wherein the user is authenticated based upon the provided first authentication data,” is indefinite “as being incomplete for omitting [the] essential step[.]” of “authenticating the user.” (Final Act. 10.) However, as Appellant argues, “this clause cannot lack the step of ‘authenticating the user’ as alleged because this is the very clause that is authenticating the user.” (Appeal Br. 19.)

In addition, the Examiner concludes that the claim 1 limitation, “wherein the user is authenticated based upon the provided first authentication data prior to the initiation of the payment transaction at said merchant,” is indefinite because “it is unclear whether the user is

authenticated prior to the initiation of the payment transaction at said merchant OR the first authentication data provided prior to the initiation of the payment transaction at said merchant.” (Final Act. 10.) We agree with Appellant that it is clear that “prior to” in this context refers back to “authenticated,” not “provided.” (Appeal Br. 19.)

Accordingly, we do not sustain the Examiner’s indefiniteness rejections.

Issue Four

Appellant argues the Examiner erred in rejecting the claims as obvious because the combination of Zambelli and Fourez would not have taught or suggested the claim limitation, “providing, by the processing device, first authentication data of the user of the at least one payment account number for payment transactions with the merchant upon the mobile device entering a premises of the merchant.” (Appeal Br. 19–21.) First, Appellant argues the Examiner erred in treating the phrase “upon entering a premises of the merchant” as a conditional limitation that has no patentable effect pursuant to MPEP § 2103(l)(c). (*Id.* at 20.) We agree with Appellant that, in the context of the claims, this phrase is not conditional, but rather is descriptive of how the method and system of Appellant’s independent claims are implemented. (*Id.*)

In addition, Appellant argues the Examiner erred in relying on the disclosure in Zambelli of a user obtaining pre-authorization for a payment transaction by following a “check-in” procedure using a mobile device when entering a merchant location. (Appeal Br. 21; *see* Final Act. 11–12; Zambelli Fig. 6, ¶¶ 16, 20, 42–44.) In particular, Appellant argues that the claims require the first authentication data to be provided “*automatically*”

upon the mobile device entering the premises of the merchant, whereas the system of Zambelli requires a non-automatic check-in procedure. (*Id.*) However, this argument is not commensurate with the scope of the claims — the claims do not require such automatic operation. (Ans. 14.)

Appellant does not otherwise argue error with respect to the independent claims, and therefore we sustain the Examiner’s rejection of claims 1, 19, and 34 over Zambelli and Fourez. (Appeal Br. 22.) We also sustain the Examiner’s rejection of claims 2, 3, 6, 10, 11, 13, 15–18, 21, 23, 26–28, and 30–33, which are not argued separately with particularity.

Issue Five

Appellant argues the Examiner erred with respect to claims 5, 8, and 25 because the combination of Zambelli and Fourez would not have taught or suggested the claim requirement, “wherein identifying said location of the mobile device includes receiving, from the mobile device, information identifying a wireless local area network of the merchant upon the mobile device entering the premises of the merchant.” (Appeal Br. 22.) The Examiner relies on the disclosure in Zambelli of identifying location information using IEEE 802.11 service set identifiers. (Ans. 14–15; Zambelli ¶¶ 29, 44.) We are not persuaded the Examiner erred in relying on this disclosure.

Appellant argues the Examiner erred with respect to claims 7, 8, 25, and 35 because the combination of Zambelli and Fourez would not have taught or suggested the claim requirement, “storing, in the storage device of the managing computer system, a plurality of merchants in association with information identifying their respective wireless local area networks.” (Appeal Br. 22.) The Examiner relies on the disclosure in Zambelli of a

centralized location determination application and merchant database in a server that identifies merchants using IEEE 802.11 service set identifiers. (Final Act. 14; Zambelli Fig. 2, ¶¶ 25, 29.) We are not persuaded the Examiner erred in relying on this disclosure.

Appellant argues the Examiner erred with respect to claims 12, 14, 24, and 29 because the combination of Zambelli and Fourez would not have taught or suggested the claim requirement, “revoking, by the processing device, the authentication based upon the first authentication data of the user of the at least one payment account number for payment transactions at said merchant upon detection of said mobile device leaving said merchant's premises,” or the requirement, “revoking, by said processing device, the authentication based upon the first authentication data of the user of the at least one payment account number at said merchant after a predetermined time of inactivity at said merchant.” (Appeal Br. 23.) The Examiner relies on the disclosure in Zambelli of pre-approval expiration “within a pre-define[d] timeframe,” or “if the check-in service receives notification that the mobile device is no longer within the check-in location.” (Final Act. 15–16; Zambelli ¶ 42.) We are not persuaded the Examiner erred in relying on this disclosure.

Appellant argues the Examiner erred with respect to claim 9 because the combination of Zambelli, Fourez, and Patel would not have taught or suggested the claim requirement, “a menu displayed on the mobile device upon the mobile device entering a premises of the merchant.” (Appeal Br. 23.) Appellant argues that, even if Patel disclose use of a menu, it does not disclose displaying the menu “upon the mobile device entering a premises of the merchant.” (*Id.*) However, Appellant’s argument is

unpersuasive as directed to Patel alone, whereas the Examiner relies on the combination of Zambelli, Fourez, and Patel. *In re Keller*, 642 F.2d 413 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091 (Fed. Cir. 1986).

Therefore, we sustain the rejection of claim 9 as obvious over the combination of Zambelli, Fourez, and Patel. We also sustain the rejection of claim 10 as obvious over the combination of Zambelli, Fourez, and Patel, as that rejection is not argued separately with particularity.

CONCLUSION

For the reasons stated above, we sustain the rejections of claims 1–3, 5–19, 21, and 23–35 pursuant to 35 U.S.C. §§ 101 and 103, and do not sustain the Examiner’s rejections based on 35 U.S.C. § 112, first and second paragraphs.

DECISION SUMMARY

In summary:

Claims Rejected	35 U.S.C. §	Reference(s)/Basis	Affirmed	Reversed
1–3, 5–19, 21, 23–35	101	Eligibility	1–3, 5–19, 21, 23–35	
1–3, 5–19, 21, 23–35	112	Written Description		1–3, 5–19, 21, 23–35
1–3, 5–19, 21, 23–35	112	Indefiniteness		1–3, 5–19, 21, 23–35
1–3, 5–8, 11–19, 21, 23–35	103	Zambelli, Fourez	1–3, 5–8, 11–19, 21, 23–35	
9–10	103	Zambelli, Fourez, Patel	9–10	
Overall Outcome			1–3, 5–19, 21, 23–35	

Appeal 2018-000670
Application 13/444,263

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)(1)(iv).

AFFIRMED