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.
14/303,155	06/12/2014	Kristofer Perez	21652-00363	1230

75564 7590 09/01/2020

DANIEL M. FITZGERALD (21652)
ARMSTRONG TEASDALE LLP
7700 Forsyth Boulevard
Suite 1800
St. Louis, MO 63105

EXAMINER	
SAX, TIMOTHY P	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
09/01/2020	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):

USpatents@armstrongteasdale.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte KRISTOFER PEREZ and PEDRO J. CHAVARRIA

Appeal 2019-002640
Application 14/303,155
Technology Center 3600

Before MICHAEL J. STRAUSS, PHILLIP A. BENNETT, and SCOTT RAEVSKY, *Administrative Patent Judges*.

STRAUSS, *Administrative Patent Judge*.

DECISION ON APPEAL[1]

STATEMENT OF THE CASE

Pursuant to 35 U.S.C. § 134(a), Appellant[2] appeals from the Examiner's decision to reject claims 1–5, 7–13, 15–21 ,23, 24, 27 and 28.

[1] We refer to the Specification, filed June 12, 2014 ("Spec."); Final Office Action, mailed May 10, 2018 ("Final Act."); Advisory Action, mailed July 6, 2018 ("Advisory Act."); Appeal Brief, filed October 3, 2018 ("Appeal Br."); Examiner's Answer, mailed December 26, 2018 ("Ans."); and Reply Brief, filed February 15, 2019 ("Reply Br.").

[2] 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. 1.

Appeal Br. 1. Claims 6, 14, 22, 25, and 26 are canceled. We have jurisdiction under 35 U.S.C. § 6(b). We AFFIRM.

CLAIMED SUBJECT MATTER

The claims are directed to consumer authentication using behavioral biometrics. Spec., Title. Claim 1, reproduced below with claim element labels added in brackets and claim elements in addition to those determined to constitute judicial exceptions identified in *italics*, is illustrative of the claimed subject matter:

> l. A computer-based method for consumer authentication of payment card transactions using behavioral biometrics, *the method using a computer device including a processor and a memory*, said method comprising:
>
> [(i)] storing, for an approved cardholder that is approved to use a payment card, a plurality of different sets of behavioral biometric profile data, each set of behavioral biometric profile data associated with a different venue type;
>
> [(ii)] receiving, *from a user-interactive device*, behavioral biometric sample data of a suspect consumer collected during a payment card transaction performed using the user interactive transaction device in which the suspect consumer presents the payment card of the approved cardholder;
>
> [(iii)] receiving, *from the user-interactive transaction device*, with the behavioral biometric sample data, a venue type identifier that represents a venue type where the payment card transaction was initiated;
>
> [(iv)] determining, from the venue type identifier received with the behavioral biometric sample data, the venue type associated with the payment card transaction, wherein the determined venue type is one of a physical venue, a virtual venue, a mobile computing application venue, a kiosk-type venue, an ATM venue, and a toll booth venue;
>
> [(v)] selecting, from the plurality of stored sets of behavioral biometric profile data of the approved cardholder, a set of behavioral biometric profile data associated with a venue

> type that matches the venue type determined from the venue type identifier received with the behavioral biometric sample data;
>
> [(vi)] comparing the behavioral biometric sample data of the suspect consumer to the selected set of behavioral biometric profile data of the approved cardholder;
>
> [(vii)] computing an authentication value based at least in part on the comparing; and
>
> [(viii)] authenticating the suspect consumer as the approved cardholder based at least in part on the authentication value.

REFERENCES

The prior art relied upon by the Examiner is:

Name	**Reference**	**Date**
Ahmed	US 8,230,232 B2	July 24, 2012
Lawrence	US 2004/0024694 A1	Feb. 5, 2004
Sands	US 2004/0148526 A1	July 29, 2004
Giobbi	US 2007/0245157 A1	Oct. 18, 2007
Bayram	US 2010/0225443 A1	Sept. 9, 2010
Hegg	US 2013/0061291 A1	Mar. 7, 2013

REJECTIONS[3]

Claims 1–5, 7–13, 15–21, 23, 24, 27, and 28 stand rejected under 35 U.S.C. § 101 because the claimed invention is directed to a judicial exception without something "significantly more" than the judicial exception. Final Act. 4–8.

Claims 1, 8, 9, 16, 17, and 24 stand rejected under 35 U.S.C. § 103 as being unpatentable over Giobbi and Hegg. Final Act. 9–12.

[3] Rejections of claim 26 under 35 U.S.C. § 112(a) and claims 9–13, 15–21, 23, and 24 under 35 U.S.C. § 112(b) (Final Act. 3–4) were addressed by the Amendment filed July 6, 2018. Advisory Act. 1.

Claims 2, 3, 5, 10, 11, 13, 18, 19, 21, and 28 stand rejected under 35 U.S.C. § 103 as being unpatentable over Giobbi, Hegg, and Ahmed. Final Act. 12–15.

Claims 4, 12, and 20 stand rejected under 35 U.S.C. § 103 as being unpatentable over Giobbi, Hegg, and Lawrence. Final Act. 15.

Claims 7, 15, and 23 stand rejected under 35 U.S.C. § 103 as being unpatentable over Giobbi, Hegg, and Sands. Final Act. 16.

Claim 27 stands rejected under 35 U.S.C. § 103 as being unpatentable over Giobbi, Hegg, and Bayram. Final Act. 16–17.

STANDARD OF REVIEW

We review the appealed rejections for error based upon the issues identified by Appellant, and in light of the arguments and evidence produced thereon. *Ex parte Frye*, 94 USPQ2d 1072, 1075 (BPAI 2010) (precedential). Arguments not made are waived. *See* 37 C.F.R. § 41.37(c)(1)(iv).

OPINION

Appellant's contentions are unpersuasive of reversible Examiner error. We adopt as our own the findings and reasons set forth by the Examiner (1) in the action from which this appeal is taken and (2) in the Examiner's Answer in response to Appellant's Appeal Brief and concur with the conclusions reached by the Examiner. We highlight the following for emphasis.

REJECTION UNDER 35 U.S.C. § 101

The Examiner's Determinations

The Examiner determines "the claims are directed to the concept of performing authentication using different authentication profiles based on the location of the type of venue the user is requesting authentication from." Final Act. 6. The Examiner equates the claimed method to "concepts which were previously identified as abstract by the courts, such as 'mitigating settlement risk' . . . 'receiving, authenticating, and publishing data' . . . and 'providing restricted access to resources.'" Final Act. 6–7 (citing *Alice*[4], *EasyWeb*[5], and *Prism Techs.*[6]). The Examiner further determines "[t]hese concepts describe 'an idea of itself'[7] and/or a 'method of organizing human

[4] *CLS Bank Int'l v. Alice Corp.*, 717 F.3d 1269, 1281 (Fed. Cir. 2013) (Lourie, J., concurring), *aff'd*, 573 U.S. 208.

[5] *EasyWeb Innovations, LLC v. Twitter, Inc.*, 689 Fed. App'x 969 (Fed. Cir. 2017) ("receiving, authenticating, and publishing data" is an abstract idea.).

[6] *Prism Techs. LLC v. T-Mobile USA, Inc.*, 696 F. App'x 1014, 1016–17 (Fed. Cir. 2017) (describing the claimed "authentication server," "access server," "Internet Protocol network," "client computer device," and "database" as "indisputably generic computer components.").

[7] Although the previously recognized category of an idea of itself is not one of the currently recognized categories, it is sufficient for the purposes of the present appeal that the claimed concepts reasonably can be characterized as falling within the still-recognized category of mental processes. *See, e.g.*, MPEP § 2106.04(a)(2)(III):

> The courts have used the phrase "an idea 'of itself'" to describe an idea standing alone such as an uninstantiated concept, plan or scheme, as well as a mental process (thinking) that "can be performed in the human mind, or by a human using a pen and paper." *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1372 . . . (Fed. Cir. 2011).

activity.'" *Id.* at 7. The Examiner further determines "the claims are not directed to a specific improvement to computer functionality." *Id.* According to the Examiner

> the claims individually and in combination do not amount to significantly more than the abstract idea itself because the claims do not effect an improvement to another technology or technical field; the claims do not amount to an improvement to the functioning of an electronic device itself which implements the abstract idea (e.g., the device, general purpose computer, and/or computer system which implements the process are not made more efficient or technologically improved); the claims do not perform a transformation or reduction of a particular article to a different state or thing (i.e., the claims do not use the abstract idea in the claimed process to bring about a physical change.[)] . . . and the claims do not move beyond a general link of the use of the abstract idea to a particular technological environment (e.g., simply claiming the use of a computer and/or computer system to implement the abstract idea).

Id. at 8 (citations omitted).

Appellant presents various arguments. Appeal Br. 5–11. We address these arguments individually in the Analysis section, below.

Principles of Law

A. SECTION 101

Inventions for a "new and useful process, machine, manufacture, or composition of matter" generally constitute patent-eligible subject matter. 35 U.S.C. § 101. However, the U.S. Supreme Court has long interpreted

Characterizing the abstract idea as a mental process instead of an idea standing alone (i.e., an idea of itself) does not constitute a change to the thrust in the Examiner's rejection.

35 U.S.C. § 101 to include implicit exceptions: "[l]aws of nature, natural phenomena, and abstract ideas" are not patentable. *Alice Corp. v. CLS Bank Int'l*, 573 U.S. 208, 216 (2014).

In determining whether a claim falls within an excluded category, we are guided by the Court's two-step framework, described in *Mayo Collaborative Services v. Prometheus Laboratories, Inc.*, 566 U.S. 66 (2012), and *Alice*. *Alice*, 573 U.S. at 217–18 (citing *Mayo*, 566 U.S. at 75–77). In accordance with that framework, we first determine what concept the claim is "directed to." *See Alice*, 573 U.S. at 219 ("On their face, the claims before us are drawn to the concept of intermediated settlement, *i.e.*, the use of a third party to mitigate settlement risk."); *see also Bilski v. Kappos*, 561 U.S. 593, 611 (2010) ("Claims 1 and 4 in petitioners' application explain the basic concept of hedging, or protecting against risk.").

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*, 561 U.S. at 611); mathematical formulas (*Parker v. Flook*, 437 U.S. 584, 594–95 (1978)); and mental processes (*Gottschalk v. Benson*, 409 U.S. 63, 67 (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 (1854))); and manufacturing flour (*Benson*, 409 U.S. at 69 (citing *Cochrane v. Deener*, 94 U.S. 780, 785 (1876))).

In *Diehr*, the claim at issue recited a mathematical formula, but the Court held that "a claim drawn to subject matter otherwise statutory does not become nonstatutory simply because it uses a mathematical formula." *Diehr*, 450 U.S. at 187; *see also id.* at 191 ("We view respondents' claims as nothing more than a process for molding rubber products and not as an attempt to patent a mathematical formula."). Having said that, the Court also indicated that a claim "seeking patent protection for that formula in the abstract . . . is not accorded the protection of our patent laws, and this principle cannot be circumvented by attempting to limit the use of the formula to a particular technological environment." *Id.* at 191 (citing *Benson* and *Flook*); *see also, e.g., id.* at 187 ("It is now commonplace that an *application* of a law of nature or mathematical formula to a known structure or process may well be deserving of patent protection.").

If the claim is "directed to" an abstract idea, we turn to the second step of the *Alice* and *Mayo* framework, where "we must examine the elements of the claim to determine whether it contains an 'inventive concept' sufficient to 'transform' the claimed abstract idea into a patent-eligible application." *Alice*, 573 U.S. at 221 (internal quotation marks omitted). "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].'" *Id.* (alterations in original) (quoting *Mayo*, 566 U.S. at 77). "[M]erely requir[ing] generic computer implementation[] fail[s] to transform that abstract idea into a patent-eligible invention." *Id.*

B. USPTO SECTION 101 GUIDANCE

In January 2019, the U.S. Patent and Trademark Office ("USPTO") published revised guidance on the application of 35 U.S.C. § 101. *See*

2019 Revised Patent Subject Matter Eligibility Guidance, 84 Fed. Reg. 50 (Jan. 7, 2019) ("2019 Guidance"), *updated by* USPTO, *October 2019 Update: Subject Matter Eligibility* (available at https://www.uspto.gov/sites/default/files/documents/peg_oct_2019_update.pdf) ("October 2019 Guidance Update"); *see also* October 2019 Patent Eligibility Guidance Update, 84 Fed. Reg. 55,942 (Oct. 18, 2019) (notifying the public of the availability of the October 2019 Guidance Update). "All USPTO personnel are, as a matter of internal agency management, expected to follow the guidance." 2019 Guidance, 84 Fed. Reg. at 51; *see also* October 2019 Guidance Update at 1.

Under the 2019 Guidance, we first look to whether the claim recites the following:

> (1) any judicial exceptions, including certain groupings of abstract ideas (i.e., mathematical concepts, certain methods of organizing human activities 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)).

2019 Guidance, 84 Fed. Reg. at 52–55.

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

> (3) adds a specific limitation beyond the judicial exception that is not "well-understood, routine, [and] 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.

2019 Guidance, 84 Fed. Reg. at 56.

Analysis

STEP 2A, PRONG 1

Under step 2A, prong 1, of the 2019 Guidance, we first look to whether the claim recites any judicial exceptions, including certain groupings of abstract ideas (i.e., mathematical concepts, certain methods of organizing human activities such as a fundamental economic practice, or mental processes). 2019 Guidance, 84 Fed. Reg. at 52–54.

Limitation (i) recites "storing, for an approved cardholder that is approved to use a payment card, a plurality of different sets of behavioral biometric profile data, each set of behavioral biometric profile data associated with a different venue type" (hereinafter "storing limitation (i)"). Appeal Br. 19, Claim App'x. Appellant directs attention to paragraph 55 of the Specification in support of this limitation. Appeal Br. 2. The cited portion of the Specification indicates behavior profiles may be stored in various systems including "a system associated with issuer . . . . , [an] interchange network . . . , [a] merchant bank . . . , or some other third party processor." Spec. ¶ 55. An approved cardholder is described as "a person that is approved by the issuer to use the card." Spec. ¶ 16.

The Specification further describes:

> As used herein, the terms "behavioral biometric transaction data" and "behavioral biometric sample data" are used generally to refer to the behavioral data captured during a transaction that

> may be used to compare to behavioral profile data for authentication of the suspect consumer. Further, as used herein, the terms "behavioral profile" and "behavioral biometric profile" are used generally to refer to the data (e.g., the reference sample(s)) that may be used as a reference sample to compare against a behavioral sample collected during a payment card transaction (e.g., a behavioral biometric sample).

Spec. ¶ 56.

Appellant discloses "behavioral biometric samples may include keystroke dynamics, values or features associated with an individual's operation of a keyboard or key pad" (Spec. ¶ 59) and "mouse-related behaviors ('mouse dynamics')" (Spec. ¶ 61). Behavioral data may further include timing data concerning "how long it takes [a] cardholder . . . to enter the code" (Spec. ¶ 62), "cognition-related behavioral data, or data that evinces an underlying state of mind or other behavioral characteristic that may distinguish some individuals from others," e.g., percentage and/or method of tipping (Spec. ¶ 63), "signature-related behavioral data ('signature dynamics')" (Spec. ¶ 64), and "behavioral data associated with online transactions," e.g., "how the cardholder traverses or otherwise interacts with the merchant's online site, and tendencies associated with payment type" (Spec. ¶ 65). In light of the description in the Specification, behavioral biometric data includes a wide range of behaviors including observable personal characteristics associated with a consumer. Therefore, behavioral biometric profile data reasonably constitutes information obtained by observation, that is, an activity performed in the human mind as a mental process.

In connection with the recited venue, the Specification discloses "[the] system is configured and customized to certain transaction venues or settings such as, for example, card-not-present transactions using a personal computer or mobile computing device, or in-store transactions using a point-of-sale device." Spec. ¶ 17. The Specification further discloses using a point-of-sale device in a traditional brick-and-mortar storefront setting, a particular operating system, mouse, keyboard, and web browser in a personal computer setting, and particular applications used to perform payment card transactions in a handheld computer (e.g., tablet) setting. *Id.* "[E]ach venue may present differing hardware, software, or other environmental factors for conducting the payment card transaction, each of which may present different behaviors or behavioral biometrics data from the consumer, and thus different behavioral biometric comparisons for authentication." *Id.* Thus, under a broad but reasonable interpretation, a venue includes and/or is indicated by the source of the behavioral biometric data, i.e., as determined by the Examiner, an "authentication type" (see Final Act. 9) such as, for example, in-person using a point-of-sale device or remotely using a personal computer. Identifying a venue, whether interpreted narrowly as identifying a location or broadly as identifying an authentication type, reasonably constitutes an observation performed in the human mind as a mental process.

Storing information also constitutes a mental process such as making note of a subject person's behavior in either the human mind or using pen and paper. The 2019 Guidance expressly recognizes such mental processes as constituting patent-ineligible abstract ideas. 2019 Guidance, 84 Fed. Reg. at 52; *see also* October 2019 Guidance Update at 9 ("A claim that encompasses a human performing the step(s) mentally with the aid of a pen and paper recites a mental process") (emphasis omitted). Therefore, storing limitation (i) recites a patent-ineligible abstract idea.

Furthermore, storing data about a consumer constitutes a method of mitigating risk by identifying those persons authorized to conduct business with or using resources of an entity (e.g., purchase an item using a payment card) that is a fundamental economic principle or practice. Likewise, storing data about a business's customers is a sales activity (e.g., who is authorized to purchase using a particular payment means) and involves satisfying a legal obligation (e.g., verifying the identity of a person presenting a third-party payment card) that are types of commercial or legal interactions. Both (1) fundamental economic principles or practices and (2) commercial or legal interactions are expressly recognized as certain methods or organizing human activity constituting patent-ineligible abstract ideas. 2019 Guidance, 84 Fed. Reg. at 52. Accordingly, for these additional reasons, storing limitation (i) recites a patent-ineligible abstract idea.

Limitation (ii) recites "receiving, from a user-interactive device, behavioral biometric sample data of a suspect consumer collected during a payment card transaction performed using the user interactive transaction device in which the suspect consumer presents the payment card of the approved cardholder" (hereinafter "biometric sample data receiving limitation (ii)") Appeal Br. 19, Claim App'x. As discussed above, biometric sample data includes a wide range of information about a consumer including, for example, the amount of a gratuity or tip that is left for a server. Gathering or receiving data constitutes a mental process, e.g., an observation. The 2019 Guidance recognizes mental processes, including

observations, as constituting a patent-ineligible abstract idea.
2019 Guidance, 84 Fed. Reg. at 52.

Furthermore, receiving data about a suspect customer is a common business (e.g., sales) practice conducted to verify a customer's identify prior to consummating a financial transaction. This receipt of data constitutes a method of mitigating risk that is a fundamental economic principle or practice and, *inter alia*, a sales activity that is a type of commercial or legal interaction. Both fundamental economic principles or practices and commercial or legal interactions are expressly recognized as certain methods or organizing human activity constituting patent-ineligible abstract ideas. 2019 Guidance, 84 Fed. Reg. at 52. Accordingly, biometric sample data receiving limitation (ii) recites an abstract idea.

Limitation (iii) recites "receiving, from the user-interactive transaction device, with the behavioral biometric sample data, a venue type identifier that represents a venue type where the payment card transaction was initiated" (hereinafter "venue type identifier receiving limitation (iii)"). Appeal Br. 19, Claim App'x. As discussed above, the recited venue type reasonably includes identification of the source of the behavioral biometric data, i.e., an authentication type. Receiving data indicating the venue, i.e., identification of the source of the behavioral biometric sample data, reasonably constitutes an observation that can be performed in the human mind. Therefore, venue type identifier receiving limitation (iii) constitutes a mental process, e.g., a mental observation. The 2019 Guidance recognizes mental processes, including observations, as constituting a patent-ineligible abstract idea. 2019 Guidance, 84 Fed. Reg. at 52.

Furthermore, observing how or where a suspect consumer presents a payment card is a common business practice. For example, a server in a restaurant presented with a payment card and needing to verify the identity of a suspect consumer presenting the card might identify a charge slip having a consumer's signature (i.e., an in-person type of authentication) as a source of biometric data. The server may consider biometric data available from the charge slip such whether the signature appears unusual or otherwise suspicious. Likewise, a cashier may observe whether an amount of a tip left by a suspect consumer is consistent with a gratuity or tip amount previously provided by the approved cardholder. Similarly, a credit card fraud detection or monitoring service may consider uses of a credit card occurring at locations distant from the usual places at which the credit card has been used in the past (e.g., outside the state or country of residence of the card holder) as indicative of potential fraudulent use of the card.

As illustrated by the examples above, it is a common business practice and sales activity to receive and consider information about where or how (e.g., presenting a payment card in person using a point-of-sale device versus remotely providing payment card information over the telephone or online using a personal computer) a suspect customer has presented a payment card as a method of risk mitigation. That is, to prevent fraudulent use of a payment card, a fraud monitoring service would be expected to receive information to determine if a venue providing customer identifying information is consistent with those venues used or frequented by the approved cardholder and/or what types of biometric data is available from the data source. Both (1) fundamental economic principles or practices (i.e., mitigating risk) and (2) commercial or legal interactions (i.e., sales activities or behaviors) are recognized as certain methods or organizing human activity constituting patent-ineligible abstract ideas. 2019 Guidance, 84 Fed. Reg. at 52. Accordingly, for this additional reason, venue type identifier receiving limitation (iii) recites an abstract idea.

Limitation (iv) recites

> determining, from the venue type identifier received with the behavioral biometric sample data, the venue type associated with the payment card transaction, wherein the determined venue type is one of a physical venue, a virtual venue, a mobile computing application venue, a kiosk-type venue, an ATM venue, and a toll booth venue

(hereinafter "determining limitation (iv)"). Appeal Br. 19, Claim App'x. Appellant's Specification does not provide details about the structure, format, or content of the recited venue type identifier other than to indicate "authentication system 650 may implement a venue type identifier for various types of venues, and behavioral data may be submitted with that venue type, or the venue type may be determined by authentication system 650 based on the type of behavioral biometric data received." Spec. ¶ 67. Determining from a venue type identifier a venue type reasonably constitutes an observation or evaluation (e.g., associating or correlating data) that can be performed in the human mind or with pen and paper. Accordingly, determining limitation (iv) constitutes a mental process that the 2019 Guidance recognizes as constituting a patent-ineligible abstract idea. 2019 Guidance, 84 Fed. Reg. at 52.

Limitation (v) recites "selecting, from the plurality of stored sets of behavioral biometric profile data of the approved cardholder, a set of behavioral biometric profile data associated with a venue type that matches the venue type determined from the venue type identifier received with the behavioral biometric sample data" (hereinafter "selecting limitation (v)") Appeal Br. 19, Claim App'x. Selecting data associated with provided key data (e.g., biometric profile data based on venue data) can be performed in the human mind as an observation, evaluation, or using judgment. As such, selecting limitation (v) constitutes a mental process recognized as a patent-ineligible abstract idea. 2019 Guidance, 84 Fed. Reg. at 52. Furthermore, selecting biometric profile data (e.g., associating a cardholder's past tipping practices with a tip indicated on a credit card charge tendered by a suspect consumer) constitutes a method of risk mitigation and/or a sales activity. Both (1) fundamental economic principles or practices and (2) commercial or legal interactions are recognized as certain methods of organizing human activity constituting patent-ineligible abstract ideas. *Id.* Accordingly, for this additional reason, selecting limitation (v) recites an abstract idea.

Limitation (vi) recites "comparing the behavioral biometric sample data of the suspect consumer to the selected set of behavioral biometric profile data of the approved cardholder" (hereinafter "comparing limitation (vi)"). Appeal Br. 19, Claim App'x. Comparing data constitutes an observation, evaluation, or judgment that can be performed in the human mind as a mental process. Therefore, in accordance with the 2019 Guidance, comparing limitation (vi) recites a patent-ineligible abstract idea.
2019 Guidance, 84 Fed. Reg. at 52.

Limitation (vii) recites "computing an authentication value based at least in part on the comparing" (hereinafter "computing limitation (vii)"). Appeal Br. 19, Claim App'x. Appellant's Specification indicates that, as an alternative to providing a discrete determination of authentication (e.g., failure or success) "authentication system 650 provides an authentication score (value) that may be used by an interchange network or other related party as a factor on whether or not to authenticate or authorize the transaction." Spec. ¶ 70. Other than describing that "the composure or factors used to generate the authentication score may depend on availability of behavioral data 626 within the particular transaction" (*id.*), Appellant does not provide details concerning the recited authentication value computation or of the format or content of the value. Therefore, consistent with a reasonable interpretation of the recited computation, determining an authentication value, i.e., a match confidence level, can be performed in the human mind or with pen and paper. Accordingly, computing limitation (iv) constitutes a mental process that the 2019 Guidance recognizes as constituting a patent-ineligible abstract idea. 2019 Guidance, 84 Fed. Reg. at 52.

Limitation (viii) recites "authenticating the suspect consumer as the approved cardholder based at least in part on the authentication value" (hereinafter "authenticating limitation (viii)"). Appeal Br. 19, Claim App'x. Appellant's Specification describes a fixed or computed threshold value may be used to determine whether an authentication value is sufficient to authenticate a suspect consumer is an approved cardholder. Spec. ¶ 71. Determining whether a value satisfies a threshold criteria can be performed in the human mind. Accordingly, authenticating limitation (viii) constitutes a mental process that the 2019 Guidance recognizes as constituting a patent-ineligible abstract idea. 2019 Guidance, 84 Fed. Reg. at 52.

We further note a determination that claim 1 recites a judicial exception to patent eligibility is consistent with Office Guidance and case law. *See* Revised Guidance, 84 Fed. Reg. at 52; *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1371–72 (Fed. Cir. 2011) (concluding claims directed to "detecting credit card fraud based on information relating to past transactions" can be performed in the human mind and were drawn to a patent-ineligible mental process); *FairWarning IP, LLC v. Iatric Systems, Inc.*, 839 F.3d 1089, 1093–94 (Fed. Cir. 2016) (concluding claims directed to "collecting and analyzing information to detect misuse and notifying a user when misuse is detected" to be mental processes within the abstract-idea category); *Inventor Holdings, LLC v. Bed Bath & Beyond, Inc.*, 876 F.3d 1372, 1378–79 (Fed. Cir. 2017) (processing of payments is a fundamental economic practice); *Zuili v. Google LLC*, 722 F. App'x 1027, 1029–31 (Fed. Cir. 2018) (unpublished) (holding ineligible claims directed to abstract ideas of collecting, transmitting, analyzing, and storing data to detect fraudulent and/or invalid clicks based on the time between two requests by the same device or client); *Prism Techs. LLC v. T-Mobile USA, Inc.*, 696 F. App'x 1014, 1016–18 (Fed. Cir. 2017) (unpublished) (holding ineligible claims directed to the abstract process of (1) receiving identity data from a device with a request for access to resources; (2) confirming authenticity of the identity data associated with that device; (3) determining whether the identified device is authorized to access the requested resources; and (4) if authorized, permitting access to the requested resources).

For the reasons discussed above, each of limitations (i) through (viii) recites one or more judicial exceptions to patent-eligible subject matter under step 2A, prong 1, of the 2019 Guidance. *See RecogniCorp*, 855 F.3d at 1327 ("Adding one abstract idea . . . to another abstract idea . . . does not render the claim non-abstract.").

STEP 2A, PRONG 2

Under step 2A, prong 2, of the 2019 Guidance, we next analyze whether claim 1 recites additional elements that individually or in combination integrate the judicial exception into a practical application. 2019 Guidance, 84 Fed. Reg. at 53–55. The 2019 Guidance identifies considerations indicative of whether an additional element or combination of elements integrates the judicial exception into a practical application, such as an additional element reflecting an improvement in the functioning of a computer or an improvement to other technology or technical field. *Id.* at 55; MPEP § 2106.05(a).

The only additional elements beyond the recited abstract ideas are a computer including a processor and a memory and a user-interactive (transaction)[8] device. Final Act. 7. The Examiner finds the additional elements, when considered individually and as an ordered combination, "do not include [an] inventive concept." *Id.* According to the Examiner,

> The claim does not improve the functioning of any computerized device nor improves another technology or technical process, or provide meaningful limitations beyond generally linking an abstract idea to a particular technological environment or mere instructions to implement an abstract idea on a computer. In other words, the additional claimed element(s) merely serve as tools to implement and/or automate the abstract idea.

Final Act. 7–8 (citing MPEP § 2106.05).

[8] Although behavioral biometric sample data receiving limitation (ii) recites a "user-interactive device", venue type identifier receiving limitation (iii) recites a user-interactive *transaction* device (emphasis added). We do not further consider whether the two devices are the same or different, noting the Specification only discloses a "transaction device' with no mention of a "user-interactive device."

Appellant contends "the claims are directly analogous to claims expressly identified by the Office as containing significantly more than an abstract idea." Appeal Br. 7. According to Appellant, "independent Claims 1, 9, and 17 are analogous to Claims 2 and 3 of Example 35 in . . . the December 2016 Guidance." *Id.* (citing to December 2016 Subject Matter Eligibility Examples: Business Methods ("Eligibility Examples") supplement to *the 2014 Interim Guidance on Subject Matter Eligibility* available at https://www.uspto.gov/sites/default/files/documents/ieg-bus-meth-exs-dec2016.pdf). According to Appellant, similar to claims 2 and 3 of Example 35, "the present claims recite a computing device that performs authentication for payment transactions." Appeal Br. 8. Appellant argues "independent Claims 1, 9, and 17 each recite a ***combination*** of limitations that operate in a ***non-conventional*** and ***non-generic*** way to authenticate users for payment card transactions - ***the same technical field improved by Claims 2 and 3 of Example 35.***" *Id.* at 9. According to Appellant:

> [T]he present claims describe a method of performing authentication using behavioral biometric data samples without requiring expensive and impractical hardware. In particular, the present claims recite an unconventional set of limitations (i.e., a computing device that stores a plurality of different sets of behavioral biometric profile data associated with different venue types, receives behavioral biometric sample data, determines a venue type, selects a set of behavioral biometric profile data that matches the venue type, and compares the selected set of behavioral biometric sample data to the behavioral biometric profile data to authenticate a transaction) to achieve this improvement in the system functionality. Further, as explained at paragraphs [0009] and [0019], the claimed limitations solve technical problems associated with known payment systems (e.g., by eliminating the need for costly and impractical hardware to perform biometric authentication).

Id.

In response, the Examiner maintains:

> Unlike claims 2 and 3 of example 35, the pending claims do not disclose steps/functions that are more than just gathering data for comparison or security purposes. The pending claims broadly describe gathering behavioral biometric data and sending the data along with an identifier for comparison/security purposes and therefore do not provide significantly more than the abstract idea itself.

Ans. 6.

Appellant replies, arguing

> the Examiner's Answer does not provide any explanation or argument as to why performing biometric authentication without requiring the expensive and impractical hardware of known systems is not unconventional or a technical improvement. Accordingly, Appellant maintains that the present claims are directed to 'significantly more' than any alleged abstract idea under Step 2B.

Reply Br. 6.

Appellant's contentions are unpersuasive of reversible Examiner error. The only additional elements beyond the recited abstract ideas are a user-interactive (transaction) device[9] and a computer device including a processor and a memory. However, the user-interactive (transaction) device is recited only in that data is received from the device, but it is not required to affirmatively perform any actions recited in claim 1. Even if otherwise, nothing in claim 1 or Appellant's Specification reasonably indicates that anything other than generic computers need to be used to carry out the abstract idea. *See, e.g.*, Spec. ¶¶ 17, 20–22.

[9] *See* n. 8.

Moreover, even if we were to interpret the initial data storing limitation (i), and receiving limitations (ii) and (iii) narrowly such that the data exists in an electronic format and is received and stored by a computer or the like, limitations (i), (ii), and (iii) still would not integrate the recited abstract ideas into a practical application. Even under such a narrow interpretation, the steps of limitations (i), (ii), and (iii) merely would constitute insignificant extra-solution activity, i.e., pre-solution activities.

> An example of pre-solution activity is a step of gathering data for use in a claimed process, e.g., a step of obtaining information about credit card transactions, which is recited as part of a claimed process of analyzing and manipulating the gathered information by a series of steps in order to detect whether the transactions were fraudulent.

MPEP § 2106.05(g).

We also do not find persuasive Appellant's attempt to analogize claim 1 to Example 35, claims 2 and 3, in the Eligibility Examples. Appeal Br. 8–9. The analysis of claims 1, 2, and 3 in the Eligibility Examples explains that the claim steps "describe a method of fraud prevention by identity verification before proceeding with a banking transaction." Eligibility Examples 9; *see also id.* at 8, 11. The analysis of claims 1, 2, and 3 provided in the Eligibility Examples results in a determination that the claims are directed to an abstract idea. *Id.* at 8, 9, 11. Therefore, the analysis of the claims proceeds to determine whether any element, or combination of elements, is sufficient to ensure the claims amount to significantly more than the abstract idea.

Claim 1 of Example 35 recites:

> 1. A method of conducting a secure automated teller transaction with a financial institution by authenticating a customer's identity, comprising the steps of:
> obtaining customer-specific information from a bank card,
> comparing, by a processor, the obtained customer-specific information with customer information from the financial institution to verify the customer's identity, and
> determining whether the transaction should proceed when a match from the comparison verifies the authenticity of the customer's identity.

The analysis of claim 1 of the Eligibility Examples finds, in addition to the steps "that describe the abstract idea of preventing fraud through verifying a customer's identity, the claim recites the additional limitation of obtaining customer-specific information from a bank card. This additional element taken individually represents a conventional action of an ATM." *Id.* at 9.

> The combination of elements is no more than the sum of their parts, and provides nothing more than mere automation of verification steps that were in years past performed mentally by tellers when engaging with a bank customer. Mere automation of an economic business practice does not provide significantly more (i.e., provide an inventive concept).

Id. Claim 1 "also recites the additional element of a processor comparing data. This processor is no more than a generic computer component, and the comparison performed by the processor does not represent any computer function beyond what processors typically perform." (*Id.*) Thus, the Eligibility Examples explain that "claim 1 is ineligible." *Id.*

Claim 2 of Example 35 recites:

> 2. A method of conducting a secure automated teller transaction with a financial institution by authenticating a customer's identity, comprising the steps of:
>
> obtaining customer-specific information from a bank card,
>
> comparing, by a processor, the obtained customer-specific information with customer information from the financial institution to verify the customer's identity, by
>
> > generating a random code and transmitting it to a mobile communication device that is registered to the customer associated with the bank card,
> >
> > reading, by the automated teller machine, an image from the customer's mobile communication device that is generated in response to receipt of the random code, wherein the image includes encrypted code data,
> >
> > decrypting the code data from the read image, and
> >
> > analyzing the decrypted code data from the read image and the generated code to determine if the decrypted code data from the read image matches the generated code data, and
>
> determining whether the transaction should proceed when a match from the analysis verifies the authenticity of the customer's identity.

The analysis of Example 35, claim 2, finds the claim recites a number of specific interactions as part of the claimed "method of conducting a secure automated teller transaction," including "obtaining customer-specific information from a bank card," transmitting a random code "to a mobile communication device that is registered to the customer associated with the bank card," "reading, by the automated teller machine, an image [that includes encrypted code data] from the customer's mobile communication device," and "analyzing the decrypted code data . . . and the generated code to determine" if they match. *Id.* at 9–10. The analysis accompanying the example distinguishes claim 2, determined to recite patent-eligible subject matter, over ineligible claim 1, explaining:

> [T]he combination of the steps (e.g., the ATM providing a random code, the mobile communication device's generation of the image having encrypted code data in response to the random code, the ATM's decryption and analysis of the code data, and the subsequent determination of whether the transaction should proceed based on the analysis of the code data) operates in a non-conventional and non-generic way to ensure that the customer's identity is verified in a secure manner that is more than the conventional verification process employed by an ATM alone. In combination, these steps do not represent merely gathering data for comparison or security purposes, but instead set up a sequence of events that address unique problems associated with bank cards and ATMs (e.g., the use of stolen or "skimmed" bank cards and/or customer information to perform unauthorized transactions).

Id. at 10.

We find no corresponding recitation of steps that address unique problems of electronic processing of bank card transactions in Appellant's claim 1. As explained above, except for the computer hardware implementing the method, the steps of limitations (i) through (viii) can be performed in the human mind or with pen and paper and/or represent certain methods of organizing human activity. There is no requirement to provide a random code, generate an image having encrypted code data in response to the code, or decryption and analysis of the code data. Instead, Appellant's claim 1 is similar to claim 1 of Example 35 by automating a process previously conducted by a human such as when a salesperson confirms a suspect consumer is likely an approved cardholder based on observation, evaluation, and judgment applied to the suspect consumer's conduct.

Claim 3 of Example 35 recites:

> 3. A method of conducting a secure automated teller transaction with a financial institution by authenticating a customer's identity, comprising the steps of:
>
> obtaining customer-specific information from a bank card,
>
> comparing, by a processor, the obtained customer-specific information with customer information from the financial institution to verify the customer's identity, by
>
> > generating a random code and visibly displaying it on a customer interface of the automated teller machine,
> >
> > obtaining, by the automated teller machine, a customer confirmation code from the customer's mobile communication device that is generated in response to the random code, and
> >
> > determining whether the customer confirmation code matches the random code, and
>
> automatically sending a control signal to an input for the automated teller machine to provide access to a keypad when a match from the analysis verifies the authenticity of the customer's identity, and to deny access to a keypad so that the transaction is terminated when the comparison results in no match.

The analysis of claim 3 of the Eligibility Examples finds the combination of steps recited by the claim "operates in a non-conventional and non-generic way to ensure that the customer's identity is verified in a secure manner that is more than the conventional verification process employed by an ATM alone." (*Id.* at 11.) Specifically, the ATM provides a random code, the ATM obtains a confirmation code from the customer's mobile communication device, determines whether the confirmation code matches the random code, and automatically sends a control signal for the ATM to provide access to a keypad when a match verifies the customer's identity. (*Id.*) Moreover,

> the combination of obtaining information from the mobile communication device (instead of the ATM keypad) and using the customer confirmation code (instead of a PIN) to verify the customer's identity does not merely select information by content or source . . . , *but instead describes a process that differs from the routine and conventional sequence of events normally conducted by ATM verification*.

Id. (emphasis added). Thus, "[t]he additional elements in claim 3 . . . represent significantly more (*i.e.*, provide an inventive concept)," and claim 3 recites patent-eligible subject matter. (*Id.*)

In contrast, Appellant's recited generic computer and user-interactive (transaction) devices perform routine functions. We are unpersuaded Appellant's claims are technical improvements by performing biometric authentication "without expensive and impractical hardware." Appeal Br. 6. In the present instance, Appellant's claims merely automate a manual authentication process that itself can rely on human-observable biometrics (albeit, according to the claims, behavioral biometric sample data is received from, but is not necessarily detected by, a user-interactive device). Contrary to Appellant's argument, we are unable to identify a recitation of a technical solution to achieve the argued benefit of eliminating the need for special (e.g., optical and electronic) biometric sensors. *See id.* at 9. Instead, the argued improvement is to the underlying concept of "performing authentication using different authentication profiles based on the location of the type of venue the user is requesting authentication from" (Final Act. 2) rather than to the computers, networks, or other technologies and platforms used to implement the concept.

Moreover, as explained above, we find the combination of steps recited in claim 1 more closely resembles the method recited in hypothetical claim 1 of Example 35, which is an example of a patent ineligible claim, i.e., recites steps comprising "a method of fraud prevention by verifying the authenticity of the customer's identity prior to proceeding with a banking transaction, which is a 'long prevalent' business practice that bank tellers have used for many years." Eligibility Examples 7–9. Thus, we do not find Appellant's contentions with respect to Example 35 persuasive of Examiner error.

Appellant's reliance on the court's decision in *BASCOM*[10] (Appeal Br. 10) is inapposite. In *BASCOM*, the court determined that "an inventive concept can be found in the non-conventional and non-generic arrangement of known, conventional pieces." *BASCOM*, 827 F.3d at 1350. In that case, the installation of a filtering tool at a specific location, remote from the end users, with customizable filtering features specific to each end user, provided an inventive concept in that it gave the filtering tool both the benefits of a filter on a local computer and the benefits of a filter on the ISP server. *Id.* We find no analogous achievement of a technical improvement here. None of the claimed steps have been shown to address a technological problem. Accordingly, Appellant's reliance on *BASCOM* is inapposite and, therefore, unpersuasive of Examiner error.

For the reasons discussed above, Appellant does not persuade us that claim 1 is directed to an improvement in the function of a computer or to any other technology or technical field. MPEP § 2106.05(a). Nor does Appellant persuasively demonstrate that claim 1 is directed to a particular machine or transformation, or that claim 1 adds any other meaningful

[10] *BASCOM Glob. Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341 (Fed. Cir. 2016).

limitations for the purposes of the analysis under Section 101. MPEP § 2106.05(b), (c), (e). Accordingly, Appellant does not persuade us that claim 1 integrates the recited abstract ideas into a practical application within the meaning of the 2019 Guidance. *See* 2019 Guidance, 84 Fed. Reg. at 52–55.

STEP 2B

Under the 2019 Guidance, only if a claim: (1) recites a judicial exception, and (2) does not integrate that exception into a practical application, do we then look to whether the claim adds a specific limitation beyond the judicial exception that is not "well-understood, routine, conventional" in the field (*see* MPEP § 2106.05(d)); **or** simply appends well-understood, routine, conventional activities previously known to the industry, specified at a high level of generality, to the judicial exception.

The Examiner finds:

> [T]he claims fail to disclose any non-conventional computer functions. Specifically the functions of storing data and sending/receiving data have been found by the courts to be well-understood, routine, conventional activity. *See* MPEP 2106.05. As stated above, the claims broadly describe gathering behavioral biometric data and sending the data along with an identifier for comparison/security purposes and therefore do not provide significantly more than the abstract idea itself. The claims do not specify an unconventional way that the behavioral biometric sample data is received or determined and instead just broadly state that the behavioral biometric sample data is received.

Ans. 7.

Appellant contends:

> [T]he combination of elements recited in the present claims is unconventional. Here, independent Claims 1, 9, and 17 contain limitations directed to the unconventional inventive concept described in the specification. Similarly, as explained above, the present claims contain limitations directed to the unconventional inventive concept of performing authentication using behavioral biometric data samples captured from motions the consumer already has to make to conduct the transaction in the particular venue, without requiring the expensive and impractical hardware (e.g., retinal scanners) used by conventional systems to acquire biometric data. Thus, the present claims are directed to patent eligible subject matter under *Berkheimer* as well.

Appeal Br. 11 (citing *Berkheimer v. HP Inc.*, 881 F.3d 1360 (Fed. Cir. 2018)).

Appellant's contention is unpersuasive of reversible Examiner error. Appellant's Specification discloses receiving behavioral biometric sample data from a user-interactive device such as "a personal computer or mobile computing device, or in-store transactions using a point-of-sale device." Spec. ¶ 17. Thus, the information is received from a conventional computer system. In connection with the computer device implementing the claimed method steps, the computer device including a processor and a memory, Appellant discloses "[i]n an example embodiment, the system is executed on a single computer system, without requiring a connection to a sever computer, . . . the system . . . run in a Windows® [(or UNIX® server)] environment." Spec. ¶ 22. The processor is generally described at a high level as "any programmable system including systems using micro-controllers, reduced instruction set circuits (RISC), application specific integrated circuits (ASICs), logic circuits, and any other circuit or processor capable of executing the functions described herein." Spec. ¶ 20. The recited memory is likewise generally described as "including RAM memory, ROM memory, EPROM memory, EEPROM memory, and non-volatile RAM (NVRAM) memory," that is, "the types of memory usable for storage of a computer program." Spec. ¶ 21.

In view of Appellant's Specification and consistent with guidance provided in the USPTO's *Berkheimer* Memorandum,[11] claim 1 merely recites generic computer components (e.g., computer devices having processors and memories) performing generic computing functions that are well-understood, routine, and conventional (e.g., receiving data, interpreting a venue type identifier to determine a venue type, selecting and comparing data, and providing a result (i.e., authenticating a suspect consumer)). *See Alice*, 573 U.S. at 225 (the "use of a computer to obtain data, adjust account balances, and issue automated instructions; all of these computer functions are 'well-understood, routine, conventional activit[ies]' previously known to the industry") (alteration in original) (quoting *Mayo*, 566 U.S. at 71–73); *Benson*, 409 U.S. at 65 (noting that a "computer operates then upon both new and previously stored data. The general-purpose computer is designed to perform operations under many different programs."); *FairWarning*, 839 F.3d at 1096 (noting that using generic computing components like a microprocessor or user interface does not transform an otherwise abstract idea into eligible subject matter); *Mortg. Grader, Inc. v. First Choice Loan Servs. Inc.*, 811 F.3d 1314, 1324–25 (Fed. Cir. 2016) (indicating components such as an "interface" are generic computer components that do

[11] Memorandum on Changes in Examination Procedure Pertaining to Subject Matter Eligibility, Recent Subject Matter Eligibility Decision (*Berkheimer v. HP, Inc.*) (Apr. 19, 2018) available at: https://www.uspto.gov/sites/default/files/documents/memo-berkheimer-20180419.PDF ("*Berkheimer* Memo").

not satisfy the inventive concept requirement); MPEP § 2106.05(d)(II) (citing *Alice* and *Mayo*); *accord Berkheimer* Memo 3–4.

The lack of detail about the structure and functioning of the additional elements in the Specification further evidences they are well-understood, routine, and conventional. *See Berkheimer* Memo at 3 (explaining that a specification that describes additional elements "in a manner that indicates that the additional elements are sufficiently well-known that the specification does not need to describe the particulars of such additional elements to satisfy 35 U.S.C. § 112(a)" can show that the elements are well understood, routine, and conventional); *Intellectual Ventures I LLC v. Erie Indemnity Co.*, 850 F.3d 1315, 1331 (Fed. Cir. 2017) ("The claimed mobile interface is so lacking in implementation details that it amounts to merely a generic component (software, hardware, or firmware) that permits the performance of the abstract idea, i.e., to retrieve the user-specific resources.").

Appellant's contention that the claims are patent-eligible because "the combination of elements recited in the present claims is unconventional" is also not persuasive. A novel and non-obvious claim directed to a purely abstract idea is, nonetheless, patent-ineligible. *See Mayo*, 566 U.S. at 90. *See also Diamond v. Diehr,* 450 U.S. 175, 188–89 (1981) ("The 'novelty' of any element or steps in a process, or even of the process itself, is of no relevance in determining whether the subject matter of a claim falls within the § 101 categories of possibly patentable subject matter."). Furthermore, under Step 2B of our analysis, *Berkheimer* does not require a finding that *all* claim elements are well-understood, routine, and conventional. Rather, a *Berkheimer* factual finding is required for *additional* elements or a combination of additional elements *outside* of the identified abstract idea. *See Berkheimer* Memo 2 ("[T]he *Berkheimer* decision . . . does provide clarification as to the inquiry into whether an additional element (or combination of additional elements) represents well-understood, routine, conventional activity"). Here, the additional elements are generic computer components (e.g., a processor and memory) performing generic computing functions (e.g., receiving and processing data) that are well-understood, routine, and conventional.

For these reasons, we determine that claim 1 does not recite additional elements that, either individually or as an ordered combination, amount to significantly more than the judicial exception within the meaning of the 2019 Guidance. 84 Fed. Reg. at 52–55; MPEP § 2106.05(d). Accordingly, we sustain the Examiner's rejection of independent claim 1 under 35 U.S.C. § 101 as directed to a judicial exception together with the rejection of independent claims 9 and 17 and dependent claims 2–5, 7, 8, 10–13, 15, 16, 18–21, 23, 24, 27, and 28 that are not argued separately.

REJECTION UNDER 35 U.S.C. § 103(a)

The Examine finds Giobbi's secure transaction authentication system teaches behavioral biometric profile data storing limitation (i), behavioral biometric sample data receiving limitation (ii), portions of behavioral biometric profile data selecting limitation (v), and behavioral biometric data comparing, authentication computing, and authenticating limitations (vi) through (viii). Final Act. 9–10. The Examiner applies the disclosed operation of Hegg's authentication server for teaching venue type identifier receiving limitation (iii), and venue type determining limitation (iv). *Id.*

at 11. The Examiner finds Hegg's disclosure that the type of authentication to be used is dependent on a received device type identifier teaches the selection criteria of selecting limitation (v) such that, in combination with Giobbi's selection of a biometric profile appropriate to the authentication information requirements of a particular reader device, the entirety of selecting limitation (v) is taught or suggested by the combination. *Id.* at 11–12.

Appellant contends the combination of Giobbi and Hegg fails to teach venue identifier receiving limitation (iii) and venue type determining limitation (iv). Appeal Br. 11. In particular, Appellant contends:

> No combination of Giobbi and Hegg describes or suggests receiving, from a user-interactive transaction device, with behavioral biometric sample data, a venue type identifier that represents a venue type where a payment card transaction was initiated, and determining, from the venue type identifier received with the behavioral biometric sample data from the transaction device, the venue type associated with the payment card transaction, as recited in the present claims.

Id. Appellant argues "Hegg is wholly silent regarding biometrics." *Id.* at 13. According to Appellant, instead of requesting behavioral biometric sample data as recited by claim 1, Hegg discloses a request to access a web service. *Id.* "Accordingly, Hegg does not describe or suggest behavioral biometric sample data, and thus does not describe or suggest receiving a venue type identifier from a user device with behavioral biometric sample data, as recited in Claim 1." *Id.*

Appellant further contends the combination of Giobbi and Hegg is improper. Appellant argues

> Hegg is directed to authenticating devices, and is unrelated to authenticating users. Further, one of ordinary skill would have no incentive to modify device authentication methods by incorporating biometric data, because devices (as opposed to users) cannot provide biometric data or be authenticated using biometric data. Accordingly, one of skill in the art would not look to combine or modify Giobbi (which is directed to authenticating users using biometric data) with Hegg (which is directed to authenticating devices), and it would be nonsensical to receive the device type identifier used in the device authentication methods of Hegg with the biometric input described in Giobbi.

Id. (emphasis omitted).

The Examiner responds, explaining:

> The [E]xaminer does not rely on Hegg to disclose behavioral biometric sample data and instead uses Hegg to disclose the concept of receiving an identifier in a request from a device and using that identifier to determine a venue type (e.g. device type) used to determine which biometric profile data (e.g. authenticator module) to use for the authentication.

Ans. 7–8 (citing Hegg ¶¶ 39–40). The Examiner continues, explaining, rather than Hegg, the Examiner relies on Giobbi for teaching storing multiple biometric profiles for a user and selecting a specific profile for authentication purposes based on the type of biometric data received from a terminal. *Id.* at 8 (citing Giobbi ¶¶ 11, 37, 38, 61, 65, 70, 77, 79). According to the Examiner, "the expression 'behavioral biometric transaction data' is not a lexicographer term and therefore the biometric data (e.g. fingerprint, voice, etc.) in Giobbi reads on the behavioral biometric transaction data used in the claims for authentication purposes." *Id.* Addressing Appellant's challenge to the propriety of combining the teachings of Giobbi and Hegg, the Examiner responds:

> The motivation to combine Hegg with Giobbi is to allow a user to execute transactions on multiple devices that all support different types of biometric authentication data. This will increase the convenience for the user since they won't have to create multiple accounts for each type of biometric authentication separately.

Id.

Appellant replies, emphasizing, because Hegg authenticates devices rather than users, Hegg does not collect biometric data for authentication purposes. Reply Br. 6. Therefore, Appellant argues, "Hegg does not disclose using an identifier to determine ***which biometric profile data to use for authentication***." *Id.* at 6–7. Appellant further argues Hegg's device type identifier fails to teach the recited venue type identifier. *Id.* at 7. "Specifically, the venue type identifier recited in the present claims indicates ***where a user performs a transaction***, unlike the device type identifier in Hegg (***which indicates the type of device to be authenticated***)." *Id.* Appellant further alleges the combination fails to teach the requirements of venue type identifier limitation (iii), arguing both the venue type identifier and behavioral sample data must be received together. According to Appellant:

> [E]ven if Giobbi describes behavioral biometric sample data and Hegg describes a venue type identifier, as alleged by the Examiner in the Examiner's Answer, the combination of Giobbi and Hegg still fails to describe or suggest ***receiving the venue type identifier and the behavioral biometric sample data together***, as required by the present claims.

Id.

Appellant's contentions are unpersuasive of reversible Examiner error. In large part, Appellant's arguments are improperly based on an improper attack on the Hegg reference individually when the rejection is based on the combination of Giobbi and Hegg. "Non-obviousness cannot be established by attacking references individually where the rejection is based upon the teachings of a combination of references." *In re Merck & Co.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986) (citing *In re Keller*, 642 F.2d 413, 425 (CCPA 1981)). For example, Appellant's argument that "Hegg is wholly silent regarding biometrics" (Appeal Br. 13) fails to address the Examiner's finding that Giobbi, not the argued Hegg reference, teaches using behavioral biometric data to authenticate a user. Final Act. 9–10, Ans. 7–8.

We are also unpersuaded by Appellant's argument that Hegg fails to describe receiving a venue type identifier from a user device with behavioral biometric data (Appeal Br. 13) because Giobbi, not Hegg, is relied upon for teaching behavioral biometric data such that the combination teaches supplying both a venue type identifier (Giobbi) and behavioral biometric data (Hegg). For the first time in the Reply Brief, Appellant argues "Hegg still fails to describe or suggest ***receiving the venue type identifier and the behavioral biometric sample data together***, as required by the present claims." Reply Br. 7.

As an initial point, Appellant's belatedly presented argument that Hegg fails to teach receiving the venue identifier *together with* the behavioral biometric sample data is not commensurate in scope with the claims which recite "receiving, from the user-interactive transaction device, *with* the behavioral biometric sample data, a venue type identifier that represents a venue type where the payment card transaction was initiated." In interpreting the argued *with* limitation, we note that, during examination of a patent application, pending claims are given their broadest reasonable construction consistent with the specification. *In re Am. Acad. of Sci. Tech Ctr.*, 367 F.3d 1359, 1364 (Fed. Cir. 2004). Construing claims broadly during prosecution is not unfair to the applicant, because the applicant has the opportunity to amend the claims to obtain more precise claim coverage. *Acad. of Sci. Tech Ctr.*, 367 F.3d at 1364; *see also In re Skvorecz*, 580 F.3d 1262, 1267–68 (Fed. Cir. 2009) ("Applicant always has the opportunity to amend the claims during prosecution, and broad interpretation by the examiner reduces the possibility that the claim, once issued, will be interpreted more broadly than is justified." (Quoting Manual of Patent Examining Procedure § 2111)).

Appellant directs attention to paragraph 69 of the Specification for disclosing disputed venue type identifier receiving limitation (iii). Appeal Br. 2. The cited portion of the Specification discloses authentication system 650 receives behavioral data and one or more approved cardholder behavioral profiles. Paragraph 69 further discloses "[i]n some embodiments, behavioral data . . . indicates a venue type, and [the] authentication system . . . uses the venue type to identify an appropriate behavioral profile . . . for use."

Although a proper interpretation of the claims requires consistency with Appellant's Specification, a particular embodiment appearing in the written description must not be read into the claim if the claim language is broader than the embodiment. *See In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993) ("[L]imitations are not to be read into the claims from the specification."). In spite of the Specification's disclosure of an embodiment in which the behavioral data also indicates a venue type, the claims only require receiving one with the other and do not specify the relationship of that particular embodiment. In particular, the claims do not require the behavioral data include a venue type identifier or simultaneous receipt of both behavioral data and the venue type identifier. Instead, claim 1 recites two receiving steps corresponding to behavioral biometric sample data receiving limitation (ii) and venue type identifier receiving limitation (iii). Thus, under a broad but reasonable interpretation, it is sufficient that both the behavioral biometric sample data and venue type identifier be received by respective limitations (ii) and (iii), either separately or together, such that both are available (i.e., received) to enable the performance of determining limitation (iv). Therefore, behavioral biometric sample data receiving limitation (iii) is taught or suggested by the combination of Giobbi and Hegg, each disclosing receipt of the respective types of data.

We are also unpersuaded by the distinction drawn by Appellant between Hegg's authentication of devices rather than users. Appeal Br. 12. As discussed above, the rejection is based on the combination of Giobbi's authentication of users and Hegg's device (i.e., venue) type identifier. Thus, Appellant's argument does not address the Examiner's findings and, instead, is an improper attack on Hegg individually when the rejection is based on the combination of Giobbi and Hegg. Furthermore, under a broad but reasonable interpretation, a device used by a person, e.g., "user equipment" is, effectively, a proxy for the user such that authentication of the user device effectively also authenticates a person using the device, i.e., the user. In any case, authentication of an entity, whether a computer or a person, reasonably suggests a broader teaching of authenticating either or both.

Furthermore, we are unpersuaded Hegg's device type identifier does not at least suggest a venue type identifier. For example, Appellant's

Specification describes collecting behavioral biometric data from "a point-of-sale device, or a desktop or laptop computer keyboard, or a mobile computing device's physical or virtual keyboard, or from any of the *devices associated with various venues* 620 as described above." Spec. ¶ 60 (emphasis added). Thus, according to the Specification, devices are associated with venues such that identification of a device also identifies a venue.

We are also unpersuaded the combination of Giobbi and Hegg is improper because, according to Appellant, "Hegg is directed to authenticating <u>devices</u> and is unrelated to authenticating <u>users</u>." Appeal Br. 13. As explained above, authenticating a device associated with a person is nonetheless reasonably understood to include authentication of the user. Furthermore, Giobbi, not Hegg, is relied upon for teaching behavioral biometric authentication. Hegg is only relied upon for venue identification used to select appropriate processing, i.e., which of Giobbi's sets of behavioral profile data are suitable for use with an identified device or venue. Here, Appellant has not demonstrated that the Examiner's proffered combination in support of the conclusion of obviousness would have been "uniquely challenging or difficult for one of ordinary skill in the art." *Leapfrog Enters., Inc. v. Fisher-Price, Inc.*, 485 F.3d 1157, 1162 (Fed. Cir. 2007) (citing *KSR*, 550 U.S. at 420).

As discussed above, the Examiner explains combining Hegg with Giobbi provides user authentication on multiple devices avoiding the need to create multiple accounts. Final Act. 11–12, Ans. 8. Thus, based on the record before us, the Examiner has articulated reasoning with rational underpinnings sufficient to justify the legal conclusion of obviousness.

For the reasons discussed above, we are unpersuaded the Examiner erred in rejecting claim 1 under 35 U.S.C. § 103(a) over Giobbi and Hegg. Accordingly, we sustain the rejection. Appellant argues claims 8, 9, 16, 17, and 24 on the basis of claim 1. Appeal Br. 14. Claims 2–5, 7, 10–13, 15, 18–21, 23, 24, 27, and 28 are not argued separately with particularity. *Id.* at 14–17. Accordingly, we further sustain the rejections of those claims under 35 U.S.C. § 103(a).

DECISION

We affirm the Examiner's rejection of claims 1–5, 7–13, 15–21, 23, 24, 27, and 28 under 35 U.S.C. §101 as directed to a judicial exception without something "significantly more" than the judicial exception.

We affirm the Examiner's rejection of claims 1, 8, 9, 16, 17, and 24 under 35 U.S.C. § 103 over Giobbi and Hegg.

We affirm the Examiner's rejection of claims 2, 3, 5, 10, 11, 13, 18, 19, 21, and 28 under 35 U.S.C. § 103 over Giobbi, Hegg, and Ahmed.

We affirm the Examiner's rejection of claims 4, 12, and 20 under 35 U.S.C. § 103 over Giobbi, Hegg, and Lawrence.

We affirm the Examiner's rejection of claims 7, 15, and 23 under 35 U.S.C. § 103 over Giobbi, Hegg, and Sands.

We affirm the Examiner's rejection of claim 27 under 35 U.S.C. § 103 over Giobbi, Hegg, and Bayram.

DECISION SUMMARY

Claims Rejected	**35 U.S.C. §**	**Reference(s)/ Basis**	**Affirmed**	**Reversed**
1–5, 7–13, 15–21, 23, 24, 27, 28	101	Judicial Exception	1–5, 7–13, 15–21, 23, 24, 27, 28	
1, 8, 9, 16, 17, 24	103	Giobbi, Hegg	1, 8, 9, 16, 17, 24	
2, 3, 5, 10, 11, 13, 18, 19, 21, 28	103	Giobbi, Hegg, Ahmed	2, 3, 5, 10, 11, 13, 18, 19, 21, 28	
4, 12, 20	103	Giobbi, Hegg, Lawrence	4, 12, 20	
7, 15, 23	103	Giobbi, Hegg, Sands	7, 15, 23	
27	103	Giobbi, Hegg, Bayram	27	
Overall Outcome			1–5, 7–13, 15–21, 23, 24, 27, 28	

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