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.
14/659,502	03/16/2015	Francisco Martinez de Velasco Cortina	116546-613CT14	3012

27189 7590 05/10/2019
PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

EXAMINER	
OUSSIR, EL MEHDI	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
05/10/2019	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):

docketing@procopio.com
PTONotifications@procopio.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte FRANCISCO MARTINEZ DE VELASCO CORTINA and
MANFRED RIETZLER

Appeal 2017-011851
Application 14/659,502
Technology Center 3600

Before ERIC B. CHEN, NABEEL U. KHAN, and MICHAEL M. BARRY, *Administrative Patent Judges*.

BARRY, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants[1] appeal under 35 U.S.C. § 134(a) from a Final Rejection of claims 1–4 and 7–23, which constitute all pending claims (claims 5 and 6 have been cancelled). *See* Final Act. 1–2 *and* App. Br. 18–21 (Claims App'x). We have jurisdiction under 35 U.S.C. § 6(b).

We reverse.

[1] Appellants identify the Applicant, Neology, Inc. as the real party in interest. App. Br. 2.

Introduction

Appellants' disclosed embodiments and claimed invention relate generally to providing secure identification solutions. Spec. ¶ 1. Disclosed embodiments include cryptographic "credit and debit exchange keys" that provide for security of payment information and for protecting use of "personal information (e.g., biometrics) contained in [a] device." Spec. ¶ 53. A key is generated when an individual's biometric stored in the device, such as a fingerprint, is matched with the output of a biometric reader, e.g., at a point of sale. Spec. ¶¶ 65–73. Encryption using the key enables protecting both the individual's biometric information and stored payment information, such as a credit card number, for a point of sale transaction. *Id.*

Claim 1, which recites limitations for a mobile device, and claim 17, which recites analogous requirements for a method for secure transactions using a mobile device, are illustrative:

> 1. A mobile device, comprising:
>
> short range radio frequency (RF) circuitry;
>
> memory configured to store biometric authentication information and payment information;
>
> a biometric module configured to read biometric information;
>
> an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory; and
>
> a secure module configured to:
>
> generate a key when the biometric information read by the biometric reading device is determined by the

authentication module to correspond to the biometric authentication information stored in memory;

encrypt the key and the payment information stored in memory; and

provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction.

17. A method for secure transactions using a mobile device, comprising:

storing biometric authentication information and payment information in memory;

reading biometric information using a biometric reader;

determining whether the biometric information read by the biometric reader corresponds to the biometric authentication information stored in memory;

generating a key when the biometric information read by the biometric reader is determined to correspond to the biometric authentication information stored in memory;

encrypting the key and the payment information stored in memory; and

providing the encrypted key and payment information for use in a transaction.

App. Br. 18, 20 (Claims App'x).[2]

[2] There is a third independent claim—claim 10—which recites a system that includes a mobile device with the same limitations as claim 1, along with a "point of sale (POS) device" configured, *inter alia*, to receive the encrypted key and payment information from the mobile device. *See* App. Br. 19–20 (Claims App'x).

Rejections[3] and References

All pending claims stand rejected under 35 U.S.C. § 101 as directed to an abstract idea, without reciting significantly more. Final Act. 8–12; *see also id.* at 2–6.

Claims 1–4, 8–13, 15–20, 22, and 23 stand rejected as unpatentable under 35 U.S.C. § 103 over Walker (US 6,163,771; Dec. 19, 2000), Holmes (US 6,848,048 B1; Jan. 25, 2005), and Chen (US 5,590,197; Dec. 31, 1996). Final Act. 12–20; *see also id.* at 6–7.

Claims 7, 14, and 21 stand rejected as unpatentable under 35 U.S.C. § 103 over Walker, Holmes, Chen, and Voltmer (US 2002/0112177 A1; Aug. 15, 2002). Final Act. 20.

ANALYSIS

General Law for the § 101 Rejection, and The 2019 Guidance

An invention is patent-eligible if it claims a "new and useful process, machine, manufacture, or composition of matter." 35 U.S.C. § 101. The Supreme Court, however, has long interpreted 35 U.S.C. § 101 to include implicit exceptions: "[l]aws of nature, natural phenomena, and abstract ideas" are not patentable. *E.g., Alice Corp. Pty. Ltd. 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 Supreme Court's two-step framework, described in *Mayo*

[3] The Examiner rejected all pending claims based on the doctrine of nonstatutory, obviousness-type double patenting. Final Act. 21–27. In response to Appellants' representation in the Appeal Brief that a terminal disclaimer will be filed upon the indication of allowable subject matter, the Examiner agreed to hold that rejection in abeyance. App. Br. 15–16; Ans. 3. In view of this, our decision does not address that double patenting rejection.

and *Alice*. *See Alice*, 573 U.S. at 217–18 (citing *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 75–77 (2012)). In accordance with that framework, we first determine what concept the claim is "directed to." *Id.* 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, 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))).

In *Diehr*, the claim at issue recited a mathematical formula, but the Supreme 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 176; *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 Supreme 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.* (citing *Benson* and *Flook*); *see also 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 citation 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.* (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.*

The PTO recently published revised guidance on the application of § 101. *2019 Revised Patent Subject Matter Eligibility Guidance*, 84 Fed. Reg. 50–57 (Jan. 7, 2019) ("the 2019 Guidance"). According to the 2019 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)).[4]

See the 2019 Guidance at 52, 55–56. 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 the 2019 Guidance at 56.

Our Analysis

For the § 101 rejection, Appellants argue all claims together as a group, contending, that the claims are *not* directed to an abstract idea pursuant to the *Alice/Mayo* framework. App. Br. 7–12. For our analysis, we select independent claim 17 as representative. 37 C.F.R. § 41.37(c)(1)(iv).

Alice/Mayo Step One

When we assess what the claims are directed to, we must do so at the same level of generality or abstraction expressed in the claims themselves. *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1337 (Fed. Cir. 2016). Here, claim 17 recites "[a] method for secure transactions using a mobile device" by (1) "storing biometric authentication information and payment information," (2) "reading biometric information," (3) "determining whether the biometric information . . . corresponds to the [stored] biometric authentication information," (4) "generating a key when the biometric information . . . is determined to correspond to the biometric authentication

[4] All references to the MPEP are to Rev. 08.2017 (Jan. 2018).

information stored," (5) "encrypting the key and the payment information," and (6) "providing the encrypted key and payment information for use in a transaction."

Considering the steps collectively, we conclude claim 17 is directed to using biometric authentication and encryption for a secure payment transaction. This is not an abstract idea, because it is neither a mathematical concept, nor a mental process, nor a method of organizing human activity, nor a combination of those categories. *See Alice*, 573 U.S. at 216; *Mayo*, 566 U.S. at 71; *see also* the 2019 Guidance at 51–55.

Thus, the Examiner errs in determining the claims are directed to an abstract idea in step one of the *Alice/Mayo* framework. Accordingly, we do not sustain the § 101 rejection of claims 1–4 and 7–23.

A. The § 103 Rejections

In the § 103 rejection of the independent claims, the Examiner finds Walker teaches the disputed limitation of "generat[ing] a key . . . when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information," as recited. Final Act. 13, 18 (citing Walker col. 5, l. 49–col. 6, l. 38, Figs. 1–9). Appellants contend Walker does not teach the disputed limitation because Walker teaches using biometric authentication simply to allow access to the device, and any key generation is a separate process triggered when the device user subsequently requests generation of single-use credit card information. App. Br. 13–14. In other words, Appellants contend the Examiner errs because Walker does not teach generating the key *when* the biometric information is authenticated. Appellants' argument is persuasive.

The Examiner responds by finding Walker teaches that "[o]nce the biometric data is authenticated, the device generates a code which is utilized to complete a transaction." Ans. 16 (citing Walker Abstract, Figs. 1–3, 8, 9, 13, and "all related text"). The Examiner does not explain, however, nor do we discern from the record before us, how or why this finding teaches or suggests the "when" requirement of the disputed limitation.

Walker's only described purpose for biometric authentication is to access the device. *See, e.g.*, Walker Fig. 3B *and* col. 6, ll. 14–20. Walker teaches that when access is granted based on successful authentication, "the device responds by querying the cardholder on display **102** whether it should generate a single-use credit card number." Walker col. 6, ll. 20–22; *see also* col. 6, l. 60–col. 7, l. 25 (disclosing an embodiment that uses key-based encryption for generating a single-use card number). Thus, generation of a key as part of generating the single-use card number takes place only after the user provides input in response to the prompt, which in turn is only provided after the end of successful biometric authentication. Because there necessarily is a delay between the conclusion of biometric authentication and the request to generate a key, Appellants persuade us that artisans of ordinary skill would have understood that generating a key in Walker takes place *after* the biometric information is authenticated, not *when* it is authenticated (as required by the disputed limitation).

Thus, we agree with Appellants that the Examiner's findings do not establish that Walker teaches (or suggests) all requirements of the disputed limitation. Accordingly, the Examiner has not established a prima facie case of obviousness for the independent claims and, therefore, we do not sustain the § 103 rejections of claims 1, 10, and 17, and, likewise, of their dependent claims 2–4, 7–9, 11–16, and 18–23.

DECISION

We reverse the Examiner's 35 U.S.C. § 101 rejection of claims 1–4 and 7–23.

We reverse the Examiner's 35 U.S.C. § 103 rejections of claims 1–4 and 7–23.

REVERSED