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.
12/396,297	03/02/2009	Charles TATO	BCM00013US02	6025

65913 7590 05/21/2018

Intellectual Property and Licensing
NXP B.V.
411 East Plumeria Drive, MS41
SAN JOSE, CA 95134

EXAMINER	
ZELASKIEWICZ, CHRYSTINA E	

ART UNIT	PAPER NUMBER
3621	

NOTIFICATION DATE	DELIVERY MODE
05/21/2018	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):

ip.department.us@nxp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte CHARLES TATO, JOSEPH WALLACE,
GREGORY YOUNGBLOOD, MARK BUER, and REX KIANG

Appeal 2017-000624
Application 12/396,297[1]
Technology Center 3600

Before ANTON W. FETTING, BRUCE T. WIEDER, and
ROBERT J. SILVERMAN, *Administrative Patent Judges*.

SILVERMAN, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

The Appellants appeal under 35 U.S.C. § 134(a) from the Examiner's decision rejecting claims 1–10 and 15–24. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM.

---

[1] The Appellants identify Broadcom Corporation as the real party in interest. Appeal Br. 3.

ILLUSTRATIVE CLAIM

1. A method for secure transaction processing in a secure processor, comprising:

receiving a request for payment information associated with an on-line transaction with an online merchant system;

reading, in a wireless card reader integrated with the secure processor, data from a payment card issued by a financial institution;

storing the payment card data in a secure memory within the secure processor;

sending the data and a credential corresponding to the payment card to an issuing bank;

receiving a set of transaction identifiers associated with the payment card from the issuing bank in response to a validation by the issuing bank of the credential; and

communicating a transaction identifier from the set of transaction identifiers as the payment information via a secure communications channel with the online merchant system.

REJECTIONS[2]

I. Claims 1–10 and 15–24 are rejected under 35 U.S.C. § 101 as ineligible subject matter.

II. Claims 1–10, 15–19, 22, and 24 are rejected under 35 U.S.C. § 103(a) as unpatentable over Ostroff (US 2006/0190412 A1, pub. Aug. 24, 2006) and Gardner (US 2009/0153297 A1, pub. June 18, 2009).

III. Claims 20, 21, and 23 are rejected under 35 U.S.C. § 103(a) as unpatentable over Ostroff, Gardner, and Official Notice.

[2] In addition to those enumerated herein, the Final Office Action (pages 2–3) sets forth a rejection of claim 22 under 35 U.S.C. § 112, first paragraph. This rejection is withdrawn. *See* Answer 2.

FINDINGS OF FACT

We rely upon and adopt the Examiner's findings stated in the Final Office Action at pages 4–18 and the Answer at pages 3–13, except as stated otherwise in the Analysis below. Additional findings of fact may appear in the Analysis below.

ANALYSIS

Subject-Matter Eligibility

Applying the first step of the methodology delineated in *Alice Corp. Pty. Ltd. v. CLS Bank International*, 134 S. Ct. 2347, 2355 (2014), the rejection states that "[t]he claims are directed to a series of steps instructing how to process a transaction, which is an abstract idea." Final Action 4. Further, under the second *Alice* step, the claims do not include any additional elements that amount to significantly more than the identified abstract idea, because the claims involve only a general purpose computer performing basic functions of a computer. *Id.*

Alleging error in the rejection, the Appellants contend that the claims in the Appeal are not directed to an abstract idea, under the first *Alice* step, because the claims require a specific structural framework in order to operate and "the features of the present claims do not make sense outside the construct of a physical computer implementation." Appeal Br. 15–16. Similarly, the Appellants submit that, rather than being directed to an abstract idea, the present claims — like those in *DDR Holdings, LLC v. Hotels.com, LP*, 773 F.3d 1245 (Fed. Cir. 2014) — address a problem arising in the realm of computer networks. *Id.* at 16–17.

Yet, the Examiner (Answer 9) aptly refers to *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335–36 (Fed. Cir. 2016), which explains that the

first step in the *Alice* inquiry asks whether the focus of the claims is on the specific asserted improvement in computer capabilities or, instead, "on a process that qualifies as an 'abstract idea' for which computers are invoked merely as a tool." Accordingly, the Appellants' assertion that the claims only make sense in the context of the computer arts is not persuasive of error in the rejection. *See* Answer 9. Furthermore, although stated in the context of the second part of the *Alice* analysis, the Supreme Court has pointed out that, with regard to questions of subject-matter eligibility, "[t]he fact that a computer 'necessarily exist[s] in the physical, rather than purely conceptual, realm,' . . . is beside the point"; merely requiring implementation with a computer does not establish subject-matter eligibility. *Alice*, 134 S. Ct. at 2358–59.

The Appellants also emphasize that the claims do not attempt to preempt or tie up the use of the abstract idea. Appeal Br. 14, 16. Yet, "[w]hile preemption may signal patent ineligible subject matter, the absence of complete preemption does not demonstrate patent eligibility." *Ariosa Diagnostics, Inc. v. Sequenom, Inc.*, 788 F.3d 1371, 1379 (Fed. Cir. 2015).

As to the second *Alice* step, the Appellants contend that the claimed subject matter is patent-eligible because it solves problems related to the transmission of sensitive data over a wireless communications network (Appeal Br. 18–19) and because it "overrides the routine and conventional sequence of events performed when processing a transaction with an online merchant and thus provide *significantly* more than what was well-understood, routine and conventional in the field" (*id.* at 20–21 (citing *DDR Holdings*, 773 F.3d at 1258)). "Specifically," the Appellants contend, "while prior art systems suffered from vulnerabilities and allowed a user's

sensitive data to be stolen and compromised, the secure processor of the instant application overrode the conventional processing by never exposing data to a network in clear text form." *Id.* at 21. *See also id.* at 19 (quoting Spec. ¶ 38[3]) ("Specifically, the instant application solved the technological problems by creating 'a secure processor (e.g., included in a security chip embedded in a computing device or in an external device) [that] is used as a reader for credit or debit card data.'")

Yet, the Appellants do not show that any claim elements (or combination thereof) amounts to significantly more than the abstract idea itself, as *Alice* requires. *See Alice*, 134 S. Ct. at 2355. In regard to the Appellants' focus on the asserted unconventional nature of claimed "secure processor," the Examiner points out that "[t]he instant claims do not describe a new wireless card reader, new secure processor, or new physical combination of the two." Answer 10.

In addition, the Appellants argue that the claim 1 "is also tied to a particular and innovative machine and thus satisfies the machine-or-transformation test." Appeal Br. 20.

Although the Supreme Court noted in *Bilski v. Kappos*, 561 U.S. 593, 604 (2010), that the machine-or-transformation test is a "useful and important clue" for determining patent eligibility of some claims, the Court, in *Mayo* emphasized that satisfying the machine-or-transformation test, by itself, is not sufficient to establish a claim as patent-eligible. *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 88 (2012). In particular, the machine-or-transformation test does not subvert the *Alice*

[3] Citations to the Specification refer to the published application, US 2009/0222383 A1, pub. Sept. 3, 2009.

analysis. *See DDR Holdings*, 773 F.3d at 1256 ("[S]atisfying the machine-or-transformation test, by itself, is not sufficient to render a claim patent-eligible, as not all transformations or machine implementations infuse an otherwise ineligible claim with an 'inventive concept.'")

Although the Appellants refer to some distinctions in the claim language among independent claims 1, 15, 17, 18, and 24 (*see* Appeal Br. 15, 19), the Appellants do not present any separate arguments based upon any of the distinctions. Accordingly, in view of the foregoing, we are not persuaded of error in the rejection of any of independent claims 1, 15, 17, 18, and 24. The Appellants present no separate argument for any of the dependent claims. Therefore, we sustain the rejection of independent claims 1, 15, 17, 18, and 24, and claims 2–10, 16, and 19–23 depending therefrom, under 35 U.S.C. § 101.

Obviousness

1. Claims 1–10, 15–17, and 22–24

The Appellants argue that independent claim 1 was rejected erroneously because the cited Ostroff reference does not teach or suggest the recited "receiving a set of transaction identifiers associated with the payment card from the issuing bank in response to a validation by the issuing bank of the credential." Appeal Br. 22–23. Specifically, the Appellants contend that, contrary to the rejection, "in Ostroff, the Cybercoupon is generated in response to a user command rather than in response to a validation by the issuing bank of a credential, as required by" claim 1. *Id.* at 23.

However, the Appellants' argument conflates different embodiments described in Ostroff and their associated "Cybercoupons" and "Cybercodes."

Thus, the Appeal Brief does not accurately reflect the way that the rejection characterizes Ostroff's disclosure.

Regarding the identified limitation of claim 1, the Examiner (*see* Final Action 5, Answer 11–12) relies upon the operation of Ostroff's "Cybercodes" (described in Ostroff ¶¶ 121–23) — *not* the "Cybercoupons" that the Appellants identify (Appeal Br. 22–23 (citing Ostroff ¶¶ 25, 26, 75, 79, 86)). According to the Examiner's Answer, Ostroff teaches the identified limitation of claim 1, because "Ostroff . . . discloses receiving a set of transaction identifiers (list of Cybercodes, see [0121-0123]) associated with the payment card from the issuing bank in response to a validation by the issuing bank of the credential (transaction approved by card issuer C, see [0079, 0094, 0098])." Answer 11–12. *See also* Final Action 5.

Rather than being generated in response to a user command — as the Appellants contend (*see* Appeal Br. 22–23), in regard to the identified Cybercoupons — portions of Ostroff cited in the rejection disclose a list of Cybercodes generated at the card issuer's location and sent to the user. *See* Ostroff ¶¶ 121–23. Therefore, the Appellants do not show that Ostroff fails to teach or suggest claim 1's recitation of "receiving a set of transaction identifiers associated with the payment card from the issuing bank in response to a validation by the issuing bank of the credential."

Accordingly, the Appellants' argument is not persuasive of error in the rejection of independent claim 1.

Because the Appellants rely upon the same argument, with regard to independent claims 15, 17, and 24 (*see* Appeal Br. 21–23), we are also not persuaded of error in the rejection of these claims. The Appellants present no separate argument, as to any of the claims depending from independent

claims 1, 15, 17, and 24. *See id.* at 24–25. Therefore, we sustain the rejections of claims 1–10, 15–17, and 22–24 under 35 U.S.C. § 103(a).

2. Claims 18–21

Independent claim 18 recites, in relevant part, "generating, using a cryptographic algorithm that combines the payment card data and a time of the on-line transaction, a one-time passcode in a one-time passcode generator within the secure processor as an identifier for the online transaction."

The Appellants contend that claim 18 was rejected erroneously, because paragraph 79 of Ostroff does not teach or suggest "using a cryptographic algorithm." Appeal Br. 24. Instead, the Appellants assert that paragraph 79 refers to generating a Cybercoupon with a card 10 that contains user program 12. *Id.*

Yet, the Appellants' argument is not persuasive of error in the rejection, because Ostroff's paragraph 79 states that user program 12 is "an Encryption Program." Accordingly, the Appellants do not show that Ostroff fails to teach or suggest "using a cryptographic algorithm," as recited in claim 18.

Therefore, we sustain the rejection of claim 18, along with claims 19–21 depending therefrom, under 35 U.S.C. § 103(a).

DECISION

We AFFIRM the Examiner's decision rejecting claims 1–10 and 15–24 under 35 U.S.C. § 101.

We AFFIRM the Examiner's decision rejecting claims 1–10 and 15–24 under 35 U.S.C. § 103(a).

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

AFFIRMED