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.
12/778,638	05/12/2010	Patrick Faith	79900-769587(045210US)	6817

66945 7590 03/30/2018

KILPATRICK TOWNSEND & STOCKTON LLP/VISA
Mailstop: IP Docketing - 22
1100 Peachtree Street
Suite 2800
Atlanta, GA 30309

EXAMINER
MANDEL, MONICA A

ART UNIT	PAPER NUMBER
3621	

NOTIFICATION DATE	DELIVERY MODE
03/30/2018	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):

ipefiling@kilpatricktownsend.com
EDurrell@kilpatricktownsend.com
KTSDocketing2@kilpatrick.foundationip.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte PATRICK FAITH
and
KRISHNA PRASAD KOGANTI

Appeal 2016-008020
Application 12/778,638
Technology Center 3600

Before CARLA M. KRIVAK, HUNG H. BUI, and
JON M. JURGOVAN, *Administrative Patent Judges*.

KRIVAK, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants appeal under 35 U.S.C. § 134(a) from a Final Rejection of claims 1, 3, 6–8, 10, 13, 14, 22, and 24–26. Claims 16–21 have been withdrawn from consideration, and claims 2, 4, 5, 9, 11, 12, 15, and 23 have been cancelled. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm-in-part.

STATEMENT OF THE CASE

Appellants' invention is directed to methods and systems by which "a portion of a real account number is encrypted," and "[t]he encrypted portion of the account number is used to generate a new account number, a new expiration date, and a new verification value" (Abstract). Appellants' invention "make[s] it more difficult to obtain numbers that can be used to conduct fraudulent transactions" because "real account information is not sent from [a] merchant to [a] payment processing network"; rather, "[t]he new account number, the new expiration date, and the new verification value can be used in a payment transaction" (Abstract).

Claims 1, 8, and 22 are independent. Independent claim 1, reproduced below, is exemplary of the subject matter on appeal.

> 1. A method comprising:
>
> encrypting, using a processor, a first portion of a first account number, the first portion having less digits than the whole first account number, to form an encrypted account number portion, while leaving a remaining portion of the first account number unencrypted, the first account number being associated with a first expiration date and a first verification value;
>
> determining a second account number based at least in part on a first segment of the encrypted account number portion and the remaining portion of the first account number;
>
> determining a second expiration date based at least in part on a second segment of the encrypted account number portion;
>
> determining a second verification value based at least in part on a third segment of the encrypted account number portion; and
>
> participating in a transaction with respect to an account corresponding to the first account number utilizing the determined second account number, the determined second expiration date and the determined second verification value in

> place of the first account number, the first expiration date and the first verification value,
>
> wherein (i) each segment of the encrypted account number portion contains less information than the whole encrypted account number portion and (ii) the first segment, the second segment and the third segment of the encrypted account number portion collectively contain all the information in the whole encrypted account number portion.

REFERENCES and REJECTIONS

The Examiner rejected claim 24 under 35 U.S.C. § 112, second paragraph.

The Examiner rejected claims 8, 10, 13, and 14 under 35 U.S.C. § 101 as directed to *signals per se*.[1]

The Examiner rejected claims 1, 3, 6–8, 10, 13, 14, 22, and 24–26 under 35 U.S.C. § 101 as directed to non-statutory subject matter that is a judicial exception without significantly more.[2]

The Examiner rejected claims 1, 3, 6–8, 10, 13, 14, 22, and 24–26 under 35 U.S.C. § 102(b) as anticipated by von Mueller (US 2008/0091944 A1; published Apr. 17, 2008).

ANALYSIS

Rejection of claim 24 under 35 U.S.C. § 112, second paragraph

The Examiner rejected claim 24 under 35 U.S.C. § 112, second paragraph as indefinite because claim 24 depends from a cancelled claim

---

[1] This rejection is presented for the first time in the Examiner's Answer (*see* Ans. 2–3, "NEW GROUNDS OF REJECTION").

[2] This rejection is presented in both the Final Action (*see* Final Act. 2) and the Examiner's Answer (under "NEW GROUNDS OF REJECTION," *see* Ans. 2–3).

(claim 4) (Final Act. 3). Appellants acknowledge "[c]laim 24 recites dependency from a canceled claim," and "invite[] an Examiner's amendment such that claim 24 depends from claim 1" (App. Br. 15). Because such amendment has not yet been entered, and Appellants have not identified error with the Examiner's § 112, second paragraph rejection, we summarily sustain the Examiner's rejection of claim 24 under 35 U.S.C. § 112, second paragraph.

Rejection of claims 8, 10, 13, and 14 under 35 U.S.C. § 101

The Examiner rejected claims 8, 10, 13, and 14 under 35 U.S.C. § 101 as directed to "***signals per se***" because these claims "are limited to 'a computer readable medium'" that "covers signals/carrier waves" (Ans. 2–3 (citing *In re Nuijten*, 500 F.3d 1346 (Fed. Cir. 2007))).

We have reviewed Appellants' Specification and do not agree with the Examiner's rejection. Initially we note the Examiner has not stated why or where the computer readable medium includes signals. Further, Appellants' Specification indicates the "computer readable medium" (e.g., as claimed in claim 8) is "a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM" (*see* Spec. ¶ 94; *see also* Spec. ¶¶ 61, 84). Thus, Appellants' claimed "computer readable medium" *does not cover* transitory propagating signals *per se*. Accordingly, we do not sustain the Examiner's rejection of independent claim 8 and its dependent claims 10, 13, and 14 under 35 U.S.C. § 101 as directed to signals *per se*.

Rejection of claims 1, 3, 6–8, 10, 13, 14, 22, and 24–26 under 35 U.S.C. § 101

In rejecting claims 1, 3, 6–8, 10, 13, 14, 22, and 24–26 under 35 U.S.C. § 101, the Examiner finds the claims are directed to "the abstract idea of determining account information based on mathematical analysis and 'participating in a transaction'" analogous or similar to abstract ideas of calculating numbers based on mathematical relationships, organizing information through mathematical correlations, collecting and comparing known information, and organizing human activity or performing processes using pen and paper (Final Act. 2; Ans. 4, 7–8, 18 (citing *Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 709, 715–16 (Fed. Cir. 2014), *Gottschalk v. Benson*, 409 U.S. 63, 71–72 (1972), *SmartGene, Inc. v Advanced Biological Labs.*, 555 F. App'x 950 (Fed. Cir. 2014))).

Appellants argue claims 1, 3, 6–8, 10, 13, 14, 22, and 24–26 are not directed to the generic abstract ideas asserted by the Examiner, but rather to novel and nonobvious data structures and technical operations of a "secure transaction protocol" that employs a "determined second account number, the determined second expiration date and the determined second verification value in place of the first account number, the first expiration date and the first verification value" to "make it more difficult to obtain numbers that can be used to conduct fraudulent transactions" (Reply Br. 7, 11–12, 14; *see also* App. Br. 17, 23).

When considering whether the claims are directed to a patent ineligible concept, such as an abstract idea, "[t]he 'directed to' inquiry . . . cannot simply ask whether the claims *involve* a patent-ineligible concept, because essentially every routinely patent-eligible claim involving physical products and actions *involves* a law of nature and/or natural phenomenon."

See Enfish, LLC v. Microsoft Corp., 822 F.3d 1327, 1335–36 (Fed. Cir. 2016) (citing *Mayo Collaborative Services v. Prometheus Laboratories, Inc.*, 566 U.S. 66, 70–71 (2012)). Rather, "the 'directed to' inquiry applies a stage-one filter to claims" considered in their entirety, in light of the Specification, to ascertain whether the claims' character as a whole is directed to excluded subject matter (*id.* (citing *Internet Patents Corp. v. Active Network, Inc.*, 790 F.3d 1343, 1346 (Fed. Cir. 2015)).

We disagree with the Examiner's conclusion that the claims are directed to generic number calculations, organizing or collecting information, organizing human activity, or performing processes using pen and paper (Final Act. 2; Ans. 4, 7–8, 18). Rather, we conclude the character of the claims as a whole is directed to an improved encryption device, such as a smartcard, and an improved encryption method for secure transaction handling (Reply Br. 12–14). *See Enfish*, 822 F.3d at 1335–36; *McRO, Inc. v. Bandai Namco Games America Inc.*, 837 F.3d 1299, 1314 (Fed. Cir. 2016) (patent eligible method claims directed to an improvement in computer animation, not an abstract idea that merely invokes generic processes and machinery).

Our conclusion is supported by the Specification's description of Appellants' invention as directed to "improved data security systems" for smartcards and other transactional consumer devices, the security systems "alter[ing] account information such as an expiration date and/or verification value" to produce a "new expiration date, . . . new verification value, . . . and . . . new account number . . . used instead of real account information to conduct payment transactions" (*see* Spec. ¶¶ 5–7, 60). The improved data security systems may be "a processor in a smartcard or a POS [point of sale]

terminal [that] can determine an existing first account number associated with a payment card and can encrypt a portion of it" as described by claims 1, 8, and 22 (*see* Spec. ¶¶ 34–35, 39, 61, 90). With Appellants' invention, "transmission of data is more secure, since real account information is not sent from [a] merchant to [a] payment processing network" (Abstract). Additionally, Appellants' invention makes it "difficult, if not impossible, for an unauthorized person to obtain the real account information associated with the user's payment card" because the encrypted "authentication elements such as expiration dates and the verification values associated with a payment card can change . . . and otherwise appear to be normal to unauthorized persons" (*see* Spec. ¶ 21).

We recognize that "collecting information, including when limited to particular content (which does not change its character as information), [is] within the realm of abstract ideas." *See Credit Acceptance Corp. v. Westlake Services*, 859 F.3d 1044, 1055–1056 (Fed. Cir. 2017) (citing *Electric Power Grp, LLC v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016)). However, as explained *supra*, the claims before us are different as they *change the character of information* via the claimed encryption operations that (i) "divid[e] an 'encrypted account number portion' into three distinct segments as part of a secure transaction protocol" and (ii) substitute the real, first account number, expiration date, and verification value by a second account number, expiration date, and verification value determined from the distinct segments (App. Br. 23; Reply Br. 12–13). Like the claims in *Enfish*, the present claims are not simply directed to any form of data encryption, but instead are specifically directed to *substitution* of a real account number, real expiration date, and real verification value by

segmented and encrypted real account number portions transformed into second account number, expiration date, and verification value, the "substitution impact[ing] on the security of the secure transaction protocol it supports" (Reply Br. 13). *See Enfish*, 822 F.3d at 1336–37 ("Here, the claims are not simply directed to *any* form of storing tabular data, but instead are specifically directed to a *self-referential* table for a computer database").

Because we find the claims are directed to eligible subject matter, we do not reach step two of the test set forth in *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 134 S. Ct. 2347, 2354 (2014). *Enfish*, 822 F.3d at 1339. Therefore, we do not sustain the Examiner's rejection of claims 1, 3, 6–8, 10, 13, 14, 22, and 24–26 under 35 U.S.C. § 101.

Rejection of claims 1, 3, 6–8, 10, 13, 14, 22, and 24–26 under 35 U.S.C. § 102(b)

The Examiner, among other things, finds von Mueller teaches "determining a second expiration date based at least in part on a second segment of the encrypted account number portion," the "encrypted account number portion" having been obtained by "encrypting . . . a first portion of a first account number, the first portion having less digits than the whole first account number," as recited in claim 1 (Ans. 11–12; Final Act. 4). Particularly, the Examiner finds von Mueller's "portion of the account number that is encrypted (PAN **406**)" teaches the claimed "encrypted account number portion" (von Mueller ¶ 274; Ans. 11), and von Mueller's paragraph 277 teaches the claimed "second expiration date" is an "updated expiration date [that] is unmistakably based on encrypted account number

since it [the account's encryption] is a prerequisite to the updating of the expiration date" (von Mueller ¶ 277; Ans. 12). We do not agree.

We agree with Appellants' arguments that von Mueller does not anticipate Appellants' claim 1 (App. Br. 12–14; Reply Br. 3–5). Particularly, we agree von Mueller's updated expiration date is not determined based on part of the *encrypted account number portion* as required by claim 1 (reciting "determining a second expiration date based at least in part on a second segment of the encrypted account number portion"). Rather, von Mueller's "'updated expiration date 410'' is merely 'a flag . . . set to provide an indication to subsequent processing equipment regarding whether the transaction data includes encrypted data'" (App. Br. 14 (citing von Mueller ¶ 277, Fig. 21)). For example, von Mueller's updated expiration date is obtained from the original "expiration date . . . *incremented by twelve years* to indicate that the transaction has been encrypted in accordance with a given encryption paradigm," such incrementing enabling "the original expiration date [to] . . . easily be recovered by reversing the [incrementing] operation" (*see* von Mueller ¶¶ 266, 277 (emphasis added)).

Thus, von Mueller's "'updated expiration date 410'' does not have a value based on a distinct *segment of 'the encrypted portion of the account number* [PAN] 406'" (App. Br. 14 (emphasis added)).

We also disagree with the Examiner's finding that von Mueller teaches segments of the encrypted account number portion, *each segment* containing *less information than the whole* encrypted account number portion, as recited in claim 1 (Ans. 10–13). Von Mueller determines secondary account number (PAN 279) and verification value (PIN 141)

using *a whole encrypted account number portion* (PAN 271' or PAN 406'), in contrast to claim 1 in which "second account number" and "second verification value" are determined from distinct *segments* where "'each segment of the encrypted account number portion contains less information than the whole encrypted account number portion'" (Reply Br. 4; *see also* App. Br. 13–14 (citing von Mueller ¶¶ 241, 243, 262, 273–280, Figs. 19 and 21)).

The Examiner has not shown, nor have we found, von Mueller determines second account number, expiration date, and verification value from respective segments "each . . . contain[ing] less information than the whole encrypted account number portion" as recited in claim 1 and similarly in claims 8 and 22. Therefore, we do not sustain the Examiner's anticipation rejection of claims 1, 8, and 22, and claims 3, 6, 7, 10, 13, 14, and 24–26 dependent therefrom. We do not address Appellants' remaining arguments with respect to dependent claims 25 and 26 as the issues discussed *supra* are dispositive of all the claims.

DECISION

The Examiner's decision rejecting claim 24 under 35 U.S.C. § 112, second paragraph is affirmed.

The Examiner's decision rejecting claims 8, 10, 13, and 14 under 35 U.S.C. § 101 as directed to signals *per se* is reversed.

The Examiner's decision rejecting claims 1, 3, 6–8, 10, 13, 14, 22, and 24–26 under 35 U.S.C. § 101 is reversed.

The Examiner's decision rejecting claims 1, 3, 6–8, 10, 13, 14, 22, and 24–26 under 35 U.S.C. § 102(b) is reversed.

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

AFFIRMED-IN-PART