Trials@uspto.gov
571-272-7822

Paper 10
Entered: September 12, 2018

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

UNIVERSAL SECURE REGISTRY LLC,
Patent Owner.

Case CBM2018-00022
Patent 9,530,137 B2

Before PATRICK R. SCANLON, GEORGIANNA W. BRADEN, and JASON W. MELVIN, *Administrative Patent Judges*.

BRADEN, *Administrative Patent Judge*.

DECISION
Denying Institution of Covered Business Method Patent Review
37 C.F.R. § 42.208

I. INTRODUCTION

This is a preliminary proceeding to decide whether, under section 18 of the Leahy-Smith America Invents Act, Pub. L. No. 112–29, 125 Stat. 284, 331 (2011) ("AIA"), a covered business method patent review of U.S. Patent No. 9,530,137 B2 (Ex. 1001, "the '137 patent" or "the challenged patent"), should be instituted under 35 U.S.C. § 324(a).[1] A covered business method patent review may not be instituted "unless . . . the information presented in the petition . . . , if such information is not rebutted, would demonstrate that it is more likely than not that at least 1 of the claims challenged in the petition is unpatentable." 35 U.S.C. § 324(a); *see* 37 C.F.R. § 42.208. We have authority under 35 U.S.C. § 324(a).

Apple Inc. filed a Petition requesting covered business method patent review of claims 1–12 of the challenged patent. Paper 3 ("Pet."). Patent Owner timely filed a Preliminary Response. Paper 8 ("Prelim. Resp."). With its Preliminary Response, Patent Owner provided evidence (Ex. 2001) that it filed with the Office a statutory disclaimer of claims 8, 10, and 11 of the '137 patent pursuant to 37 C.F.R. § 1.321(a). Prelim. Resp. 15 (citing Ex. 2001).

---

[1] *GTNX, Inc. v. INTTRA, Inc.*, 789 F.3d 1309, 1310 (Fed. Cir. 2015) (describing transitional program for review of covered business method patents, pursuant to the AIA, as subject to "'the standards and procedures of[] a post-grant review under' . . . 35 U.S.C. §§ 321–329," absent exceptions not applicable here (alteration in original) (quoting AIA § 18(a)(1))).

Upon consideration of the record, as explained in detail below, we determine that the '137 patent is not a covered business method patent and accordingly deny the Petition.

A. Related Matters

As required by 37 C.F.R. § 42.8(b)(2), each party identifies various judicial or administrative matters that would affect or be affected by a decision in this proceeding. Pet. 3–4; Paper 7, 2 (Patent Owner's Mandatory Notices).

B. The '137 Patent

The '137 patent is titled "Method and Apparatus for Secure Access Payment and Identification" and describes ways to securely authenticate the identity of a plurality of users. Ex. 1001, [54], [57], 1:43–55.

1. Written Description

The challenged patent describes a secure database called a "Universal Secure Registry," which can be used as "a universal identification system" and/or "to selectively provide information about a person to authorized users." *Id.* at 4:8–11. The '137 patent states that the USR database is designed to "take the place of multiple conventional forms of identification." *Id.* at 4:23–25. The '137 patent further states that various forms of information can be stored in the database to verify a user's identity and prevent fraud:

(1) algorithmically generated codes, such as a time-varying multi-character code or an "uncounterfeitable token," (2) "secret information" like a PIN or password, and/or (3) a user's "biometric information," such as fingerprints, voice prints, an iris or facial scan,

DNA analysis, or even a photograph. *See id.* at 14:1–7, 14:21–40, 44:54–61, Fig. 3. Accordingly, the '137 patent discloses that the system can be used to selectively provide authorized users with access to perform transactions involving various types of confidential information stored in a secure database. *See, e.g.*, *id.* at 4:8–15. "For example, a person may wish to participate in a transaction to give a potential employer one-time access to job application information 44." *Id.* at 17:11–13.

The '137 patent specifically discloses that an event enabled or prevented by the system "may be a transaction (e.g., a financial transaction), access control (e.g., physical or electronic access), or other action that is either enabled or prevented." *Id.* at 6:58–61, *see also* 28:49–50 ("[v]arious embodiments can be employed to control access to a physical facility."). Certain embodiments in the '137 patent illustrate that the transactions may provide "Address Information," "Financial Information," "Medical Information," or "Tax Information." *Id.* at 13:42–14:7, Figs. 3, 4; *see also* 15:6–57, 17:11–13, 23:18–21, 24:12–16, 24:46–49. Still other embodiments of the '137 patent disclose transactions involving "any of a wide variety of acts including: authorizing a withdrawal of money from a user's account, permitting the user access to a secure area, permitting a user to view medical information concerning themselves or a third party, or permitting the user to access other confidential information." *Id.* at 42:64–43:3.

2. Illustrative Claims

Claims 1 and 12 are independent and illustrate the challenged subject matter.

> 1. A system for authenticating a user for enabling a transaction, the system comprising:
> a first device including:
> a first processor, the first processor programmed to authenticate a user of the first device based on secret information and to retrieve or receive first biometric information of the user of the first device;
> a first wireless transceiver coupled to the first processor and programmed to transmit a first wireless signal including first authentication information of the user of the first device; and
> a biometric sensor configured to capture the first biometric information of the user;
> wherein the first processor is programmed to generate one or more signals including the first authentication information, an indicator of biometric authentication, and a time varying value in response to valid authentication of the first biometric information, and to provide the one or more signals including the first authentication information for transmitting to a second device; and
> wherein the first processor is further configured to receive an enablement signal from the second device; and
> the system further including the second device that is configured to provide the enablement signal indicating that the second device approved the transaction based on use of the one or more signals;
> wherein the second device includes a second processor that is configured to provide the enablement signal based on the indication of biometric authentication of the user of the first device, at least a portion of the first authentication information, and second authentication information of the user of the first device to enable and complete processing of the transaction.

Id. at 45:27–61.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.