Trials@uspto.gov
571-272-7822

Paper No. 9
Entered: October 9, 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 IPR2018-00809
Patent 9,530,137 B2

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

MELVIN, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

Petitioner, Apple Inc., filed a Petition (Paper 3, "Pet.") requesting *inter partes* review of claims 1, 2, and 5–12 (the "challenged claims") of U.S. Patent No. 9,530,137 B2 (Ex. 1001, "the '137 patent"). Patent Owner, Universal Secure Registry, LLC, timely filed a Preliminary Response. Paper 8 ("Prelim. Resp."). Pursuant to 35 U.S.C. § 314 and 37 C.F.R. § 42.4(a), we have authority to determine whether to institute review.

An *inter partes* review may not be instituted unless "the information presented in the petition . . . and any response . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." 35 U.S.C. § 314(a). For the reasons set forth below, we conclude Petitioner has shown a reasonable likelihood it will prevail in establishing the unpatentability of at least one challenged claim. We, therefore, institute *inter partes* review of the challenged claims.

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. 2–3; Paper 7, 2 (Patent Owner's Updated 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. 1101, [54], [57], 1:43–55.

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.

The patent discloses a variety of embodiments including those in which a user is authenticated on a device using secret information (such a PIN code) and biometric information (such as a fingerprint), then the first device transmits information to a second device for further authentication. *See id.* at 29:21-44. The second device may verify the user's information and return an enablement signal to the first device. *Id.* at 33:20–34. 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.

C. CHALLENGED CLAIMS

Challenged claims 1 and 12 are independent. Claim 1 is illustrative of the claimed subject matter and is reproduced below:

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.

Ex. 1101, 45:27–61.

D. PROPOSED GROUNDS OF UNPATENTABILITY

Petitioner asserts the following grounds of unpatentability:

Basis	Reference(s)	Claims
§ 103(a)	Jakobsson[1] and Maritzen[2]	1, 2, 6, 7, 9, 10, and 12
§ 103(a)	Jakobsson, Maritzen, and Niwa[3]	5
§ 103(a)	Jakobsson, Maritzen, and Schutzer[4]	8 and 11

Pet. 20, 53, 63. Petitioner also relies on the Declaration of Dr. Victor Shoup (Ex. 1102). Pet. 9.

E. OBVIOUSNESS OVERVIEW

An invention is not patentable "if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains." 35 U.S.C. § 103(a).[5] The question of obviousness is resolved on the basis of underlying factual determinations including: (1) the scope and content of the

[1] International Patent Application Publication No. WO 2004/051585, published June 17, 2004 (Ex. 1113).
[2] U.S. Patent Application Publication No. 2004/0236632, published November 25, 2004 (Ex. 1114).
[3] U.S. Patent No. 6,453,301, issued September 17, 2002 (Ex. 1117).
[4] European Patent Application Publication No. EP 1028401, published August 16, 2000 (Ex. 1115).
[5] The America Invents Act included revisions to, *inter alia*, 35 U.S.C. § 103 effective on March 16, 2013. Because the '137 patent claims benefit of filing date under § 120 to an application filed before March 16, 2013 (*see* Ex. 1101, 1:7–40), the pre-AIA version of 35 U.S.C. § 103 applies.

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.