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

U.S. Patent No. 9,530,137

PETITIONER'S MOTION TO STRIKE

PORTIONS OF PATENT OWNER'S PAPER 31 AND EXHIBIT 2021

Table of Contents

Page

In its Reply in further support of its Conditional Motion to Amend

("CMTA") (Paper 31) and in the accompanying expert declaration (Exhibit 2021),

the Patent Owner cites to new portions of the '660 application as part of a new

theory for written description support for claims 13 and 21 that its CMTA did not

include (Paper 19). Pursuant to Paper 34, Petitioner moves to strike this argument

and evidence.

Exhibits 1136 and 1137, submitted herewith, are versions of Paper 31 and

Exhibit 2021 that highlight the new argument and evidence that Petitioner seeks to

strike.

## I.	PATENT OWNER'S CMTA REPLY AND ITS EXPERT'S DECLARATION PRESENT NEW PURPORTED WRITTEN DESCRIPTION SUPPORT.

In its CMTA, Patent Owner proposed amending claims 13 and 21 to recite,

inter alia, the following limitations:

- 13[c]: " . . . the first authentication information including a multi-digit

  identification (ID) code allowing a networked validation-information

  entity to map the multi-digit ID code to a credit and/or debit card

  number . . ."

- 13[e]: " . . . the second device being the networked validation-information entity configured to enable the credit and/or debit card transaction based on authentication of the user . . ."

- 21[d]: ". . . the first authentication information including a multi-digit identification (ID) code allowing a networked validation-information entity to map the multi-digit ID code to a financial account number . . ."

- 21[f]: "the second device being the networked validation-information entity configured to enable the financial transaction based on authentication of the user"

CMTA at B1, B4.

As explained below, while Patent Owner's CMTA contended that these limitations are supported by an embodiment where a *USR* sends a multi-digit public code to a *credit card company*, which then performs the claimed mapping, Patent Owner now argues that these limitations are supported by a different embodiment in which a *user's electronic ID device* sends a code to a *USR*, which then allegedly performs the claimed mapping.

The CMTA contended that the limitations listed above are supported at least in part at page 23, line 34 through page 24, line 2 of the '660 application (Exhibit

2006). CMTA at 7-8. The '660 application states there that a universal secure registry ("USR") may "instead transmit[], on approval, a multidigit public ID code for the credit card holder which the credit card company can map to the correct credit card number." Exhibit 2006, 23:34-24:2. Thus, Patent Owner's originally-cited support related only to replacing transmittal of a credit card number to a credit card company with a multidigit public ID code to be mapped to a credit card number—not to any communications between a user's electronic ID device and the USR.

In Petitioner's CMTA Opposition, Petitioner demonstrated that the '660 application does not provide written description support for the proposed, amended claimed functions of the "networked validation-information entity" and the "second device" being co-located. CMTA Opposition, Paper 24, 23-24. Indeed, in the '660 application, the claimed "second device" is the disclosed USR, while the claimed "networked validation-information entity" is the disclosed credit card company. However, the '660 application does not disclose that the second device is the same entity as the networked validation-information entity proposed limitations 13[e] and 21[f] require. *See id.*

In its CMTA Reply, however, Patent Owner cites to new portions of the '660 application in an attempt to cure what Petitioner argued in its Opposition was

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.

fastcase®
Smarter legal research.