Trials@uspto.gov
Tel: 571-272-7822

Paper 7
Entered: January 15, 2016

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SPECTRUM BRANDS, INC.,
Petitioner,

v.

ASSA ABLOY AB,
Patent Owner.

Case IPR2015-01563
Patent 7,706,778

Before RAMA G. ELLURU, BEVERLY M. BUNTING, and CHRISTOPHER G. PAULRAJ, *Administrative Patent Judges.*

BUNTING, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
37 C.F.R. § 42.108

I. INTRODUCTION

Spectrum Brands, Inc. ("Petitioner") filed a Petition requesting *inter partes* review of claims 1, 4, 6, 8, 10–14, 16–18, 22–25, 28–31, 33, and 34 (the "challenged claims") of U.S. Patent No. 7,706,778 (Exhibit 1001, "the '778 patent") pursuant to 35 U.S.C. §§ 311–319. Paper 1 ("Pet."). Patent Owner, Assa Abloy AB. ("Patent Owner") waived filing of a Preliminary Response to the Petition. Paper 6. We have jurisdiction under 35 U.S.C. § 314, which provides that an *inter partes* review may not be instituted "unless . . . there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition."

Upon consideration of the information presented in the Petition, and for the reasons explained below, we determine that Petitioner has not established a reasonable likelihood that the challenged claims are unpatentable. Accordingly, we decline to institute an *inter partes* review of the challenged claims of the '778 patent.

II. BACKGROUND

A. Related Matters

The parties indicate that the '778 patent is the subject of the following district court action: *HID Global Corporation et al. v. Kwikset Corporation et al.*, No. 14-cv-00947-CJC-DFM (C.D. Cal.). Pet. 5, Paper 5, 2. Petitioner filed an additional petition requesting *inter partes* review of the following related patent: U.S. Patent No. 8,150,374 (IPR2015-01562).[1] *Id.*

[1] IPR2015-01440 and IPR2015-01441 involving the '778 patent and U.S. Patent No. 8,150,374, respectively, were both terminated pursuant to a settlement agreement.

B. The '778 Patent (Ex. 1001)

The '778 patent is directed to the use of mobile devices in an access control system to control "access to assets, places, or things by having access credentials remotely assigned and revoked." Ex. 1001, 1:20–21. As shown in Figure 1, reproduced below, the system 100 automatically and remotely updates credential information associated with the mobile device.

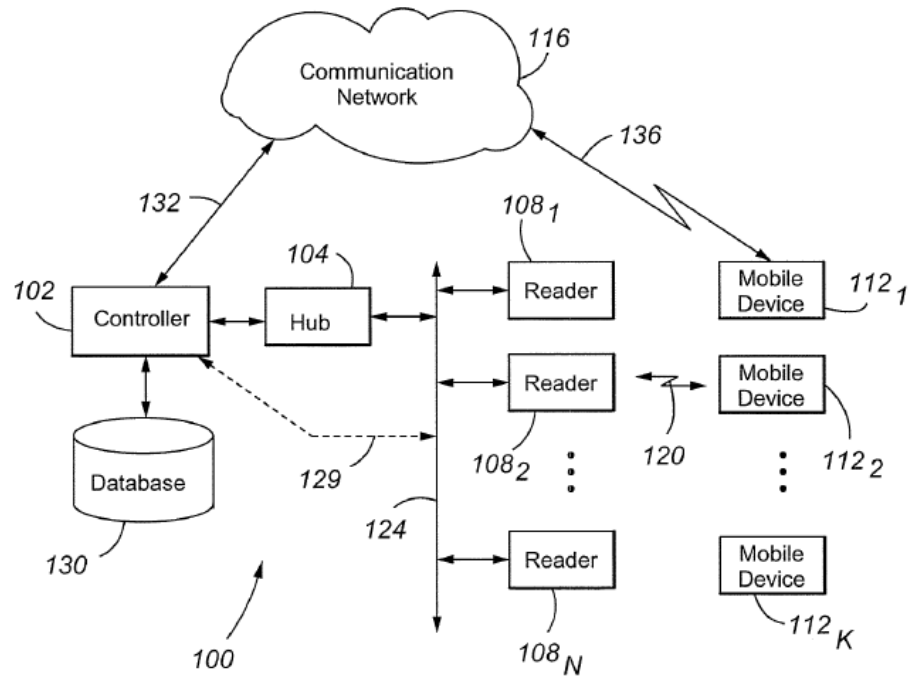

Fig. 1

Figure 1 is a diagrammatic view of a system for authenticating mobile devices and remotely updating associated credentials. *Id.* at 4:40–42.

System 100 includes controller 102 coupled to a plurality of readers 108 via interconnecting hub 104. *Id.* at 4:66–5:1. The controller also communicates with at least one of the plurality of mobile devices 112 via communication network 116. *Id.* at 6:61–63. The reader is associated with a particular asset, and "is adapted for exchanging information with the controller **102**

and for requesting data from the mobile device **112** to verify the authenticity of the mobile device." *Id.* at 6:9–13.

The mobile device contains a memory 200 that "may be selectively modified and/or erased by the controller 102 and/or the reader 108." *Id.* at 8:1–3. Identification information, including "credential information of the user of the mobile device 112, for instance, unique IDs, manufacture IDs, passwords, keys, encryption schemes, transmission protocols, and the like" is loaded into the mobile device memory. *Id.* at 8:9–12. The mobile device memory also includes self-authenticating data, e.g., "assets the mobile device **112** has access to, times of allowed access to each asset, and other data that can assist the mobile device in determining if it is eligible to gain access to a particular asset" (*Id.* at 8:22–25) and self-authenticating functions, e.g., "us[ing] the self-authenticating data to enable the mobile device **112** to make a determination of its own access rights with respect to an asset" (*Id.* at 8:25–28).

Upon presentation of the mobile device to the reader, the reader provides asset information and time of day information to the mobile device. *Id.* at 8:35–38. The mobile device analyzes the asset information and time of day information using its self-authenticating data to determine whether it is allowed to access the asset. *Id.* at 8:38–41. If the mobile device determines that it is allowed access to the asset (*Id.* at 8:44–45), it sends a signal to the reader "indicating that validation of the mobile device 112 has been confirmed and access should be granted" so that the reader allows access to the asset. *Id.* at 8:46–47.

The '778 patent further describes in Figure 3 a method for automatically and remotely updating credential information on the mobile

device. *Id.* at 9:36–39; Fig. 3. For example, if credential information used by a mobile device to verify its authenticity is changed at the controller, the memory of the mobile device is likewise updated. *Id.* at 9:40–10:6. In another embodiment of a method for automatically and remotely updating credential information on the mobile device, described in Figure 4, a time interval between credential updates is determined. *Id.* at 10:7–23. New credential information is sent to the readers and the mobile devices periodically to keep self-authenticating data and/or functions active and up to date. *Id.* at 10:51–54.

C. Illustrative Claim

Of the challenged claims, claims 1, 16 and 33 of the '778 patent are independent. Claim 1 is illustrative of the challenged claims and is reproduced below:

> 1. A method of remotely maintaining a secure access system, comprising:
>
> receiving, at a secure access system controller, a credential update for at least one user of the secure access system;
>
> in response to receiving the credential update, said controller automatically initiating a system update process, the system update process comprising:
>
> generating a message comprising information representing the credential update;
>
> determining at least one target for said message, wherein said at least one target comprises at least one mobile device associated with the at least one user; and

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.