Trials@uspto.gov
571.272.7822

Paper No. 11
Filed: May 24, 2016

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SECURUS TECHNOLOGIES, INC.,
Petitioner,

v.

JOHN D. PROFANCHIK, SR.,
Patent Owner.

Case IPR2016-00268
Patent 8,315,367 B2

Before KEVIN F. TURNER, BARBARA A. BENOIT, and GEORGIANNA W. BRADEN, *Administrative Patent Judges*.

BRADEN, *Administrative Patent Judge*.

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

I. INTRODUCTION

A. Background

Securus Technologies, Inc. ("Petitioner") filed a Petition (Paper 1, "Pet.") to institute an *inter partes* review of claims 1–20 of U.S. Patent No. 8,315,367 B2 (Ex. 1001, "the '367 patent"). On the cover of its Petition for *inter partes* review, Petitioner indicated that Global Tel*Link Corporation was the patent owner. Global Tel*Link Corporation, however, informed the Board that John D. Profanchik, Sr. is the patent owner and real party-in-interest. Paper 4, 2; Paper 5, 1. John D. Profanchik, Sr. ("Patent Owner") timely filed a Preliminary Response (Paper 5, "Prelim. Resp."). We have jurisdiction under 35 U.S.C. § 314(a), 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 Corrected Petition, the Petition's supporting evidence, Patent Owner's Preliminary Response, and Patent Owner's responsive pleading regarding amended citations found in the Corrected Petitioner (Paper 10) we conclude Petitioner has established a reasonable likelihood it would prevail with respect to at least one of the challenged claims. Accordingly, for the reasons that follow, we institute an *inter partes* review.

B. Related Proceedings

Petitioner informs us that no other related matters would affect or be affected by this proceeding. Pet. 59; *see* Paper 4, 2–3.

C. The '367 Patent

The '367 patent discloses "systems and methods for preventing unauthorized persons from using an electronic device within a facility." Ex. 1001, Abst. The '367 patent teaches a radio frequency identification (RFID) system that identifies prison inmates within an RFID coverage zone during use of the telephone. The system determines whether the phone call can continue to proceed based on the proximity of one or more inmates to the telephone. *Id.* at 1:49–53, 2:16–20.

One embodiment of the '367 patent provides an RFID access system that includes RFID tags having unique identification information associated with wearers of the RFID tags. *Id.* at 2:39–41. The RFID tag "having unique identification information associated with a wearer of the RFID tag," which may be contained in "a non-removable item worn by the wearer, such as a bracelet." *Id.* at 2:40–43. RFID tags may be constructed such that they cannot be removed and are tamperproof. *Id.* at 5:26–28. The RFID system includes a reader having an RFID coverage zone for detecting RFID tags within the zone. *Id.* at 2:43–45. One embodiment of an RFID tag reader and RFID coverage zone is illustrated in Figure 2, reproduced below.

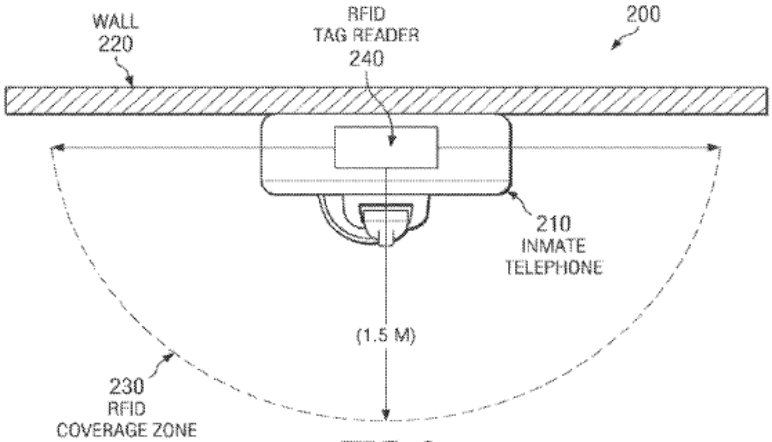
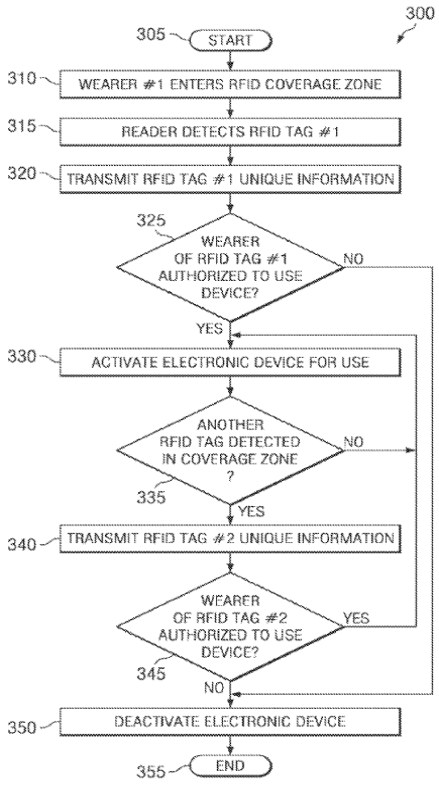


FIG. 2

As shown above in Figure 2 of the ’367 patent, system 200 includes inmate telephone 210, RFID coverage zone 230, and RFID tag reader 240. *Id.* at 5:36–38, Fig. 2. In this specific embodiment, RFID coverage zone 230 is generated around telephone 210 by RFID reader 240, which is integrated within telephone 210. *Id.* at 5:37–39.

Another embodiment of the ’367 patent provides a call management system that connects the reader and determines whether wearers in the coverage zone are authorized to use the electronic device (*e.g.*, a telephone) based on a detected RFID tag’s unique identification information. *Id.* at 2:45–50, 7:19–21, cl. 1, Fig. 3. An example of a process by which an RFID-based access management system may be used to ensure only authorized person use an electronic device in a facility is shown in Figure 3, reproduced below.



As shown above in Figure 3 of the ’367 patent at step 350, the call management system deactivates the electronic device if it determines an unauthorized wearer is detected in the coverage zone. *Id.* at 2:50–52, 3:22–26, 7:25–28, Fig. 3.

D. Illustrative Claims

As noted above, Petitioner challenges claims 1–20 of the ’367 patent, of which claims 1 and 11 are the only independent claims. Claims 1 and 11 are illustrative of the challenged claims and are reproduced below (with paragraphing):

1. An access management system for preventing unauthorized persons from using an electronic communication device in a custodial facility, the system comprising:

   a RFID tag configurable to have unique identification information that can be associated with a wearer of the RFID tag, wherein the RFID tag is configured to be comprised in a non-removable item worn by the wearer;

   a reader configurable to be associated with the electronic communication device, the reader configurable to have a RFID coverage zone for detecting RFID tags within the coverage zone; and

   a call management system configurable to be connected to the reader and configurable to determine whether a wearer is authorized to use the electronic communication device based at least in part on an RFID tag's detected unique identification information;

   wherein the reader is configured to detect when the RFID tag is within the coverage zone, the call management system activating the electronic communication device if it determines the wearer is authorized to use the electronic communication device.

Ex. 1001, 9:33–52.

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.