

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MOBILE TECH, INC.,
Petitioner,

v.

INVUE SECURITY PRODUCTS INC.,
Patent Owner.

IPR2018-01138
Patent 9,659,472 B2

Before JUSTIN T. ARBES, STACEY G. WHITE, and
DANIEL J. GALLIGAN, *Administrative Patent Judges*.

WHITE, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

We have authority to hear this *inter partes* review under 35 U.S.C. § 6. This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a). For the reasons discussed herein, we determine that Mobile Tech, Inc. (“Petitioner”) has shown, by a preponderance of the evidence, that claims 1–10 and 12–45 (“the challenged claims”) of U.S. Patent No. 9,659,472 B2 (Ex. 1001, “the ’472 patent”) are unpatentable.

A. Background

Petitioner requested *inter partes* review of the challenged claims. Paper 3 (“Petition”). InVue Security Products Inc. (“Patent Owner”) filed a Patent Owner Preliminary Response. Paper 9. Based on our review of these submissions, we instituted a trial on all of Petitioner’s challenges as described in the Petition. Paper 12 (“Dec. on Inst.”). Petitioner contends the challenged claims are unpatentable on the following grounds (Pet. 6):

Claims Challenged	35 U.S.C. §	References
1–10, 12–15, 17–32, 34–43, 45	103(a)	Rothbaum, ¹ Denison ²
16, 33, 44	103(a)	Rothbaum, Denison, Ott ³
1–10, 12–15, 17–32, 34–38, 41	103(a)	Rothbaum, Denison, Deguchi ⁴

¹ U.S. Patent 5,543,782, issued Aug. 6, 1996 (Ex. 1003, “Rothbaum”).

² U.S. Patent Pub. 2004/0201449 A1, pub. Oct. 14, 2004 (Ex. 1002, “Denison”).

³ U.S. Patent No. 6,380,855 B1, issued Apr. 30, 2002 (Ex. 1005, “Ott”).

⁴ U.S. Patent Pub. 2004/0003150 A1, pub. Jan. 1, 2004 (Ex. 1004, “Deguchi”).

Claims Challenged	35 U.S.C. §	References
16, 33	103(a)	Rothbaum, Denison, Deguchi, Ott

Patent Owner filed a Patent Owner Response (Paper 14, “PO Resp.”), Petitioner filed a Reply (Paper 17, “Reply”), and Patent Owner filed a Sur-Reply (Paper 19, “Sur-Reply”).

An oral hearing was held on August 29, 2019, and a transcript of the hearing is included in the record (Paper 24, “Tr.”). After the hearing, the parties met and conferred regarding the potential application of collateral estoppel to certain issues in this proceeding. The parties provided us with a list of their agreements and disagreements as to the application of collateral estoppel. Ex. 3001. We then authorized the parties to provide further briefing regarding the parties’ stated disagreements regarding the application of collateral estoppel to this proceeding. Paper 25. Petitioner filed a brief (Paper 26, “Pet. CE Br.”) and Patent Owner filed a responsive brief (Paper 27, “PO CE Br.”).

B. Related Proceedings

The parties indicate the ’472 patent is at issue in a series of lawsuits that have been consolidated and transferred to the United States District Court for the District of Oregon. Paper 11, 2–3; Paper 6, 1. Petitioner previously sought post-grant review of the ’472 patent (PGR2018-00004), but that petition was denied because the ’472 patent is not eligible for such review. *See* Pet. 3; PGR2018-00004, Paper 15. Petitioner has filed petitions for *inter partes* review involving the same parties and related patents, IPR2016-00892, IPR2016-00895, IPR2016-00896, IPR2016-00898,

IPR2016-00899, IPR2016-01241, IPR2016-01915, IPR2017-00344, IPR2017-00345, IPR2017-01900, IPR2017-01901, and IPR2018-00481. Paper 11, 3–4. Final written decisions have been issued in each of those *inter partes* review proceedings. To date, eight of those final written decisions have been affirmed by the Court of Appeals for the Federal Circuit. Ex. 1029. The parties also identify pending patent applications that may be affected by this proceeding. See Paper 11, 5; Paper 6, 1.

C. The '472 patent

The '472 patent describes security systems and methods involving a key programmed by a programming station with a security code. Ex. 1001, 1:30–36. This security system is illustrated in Figure 1, which is reproduced below.

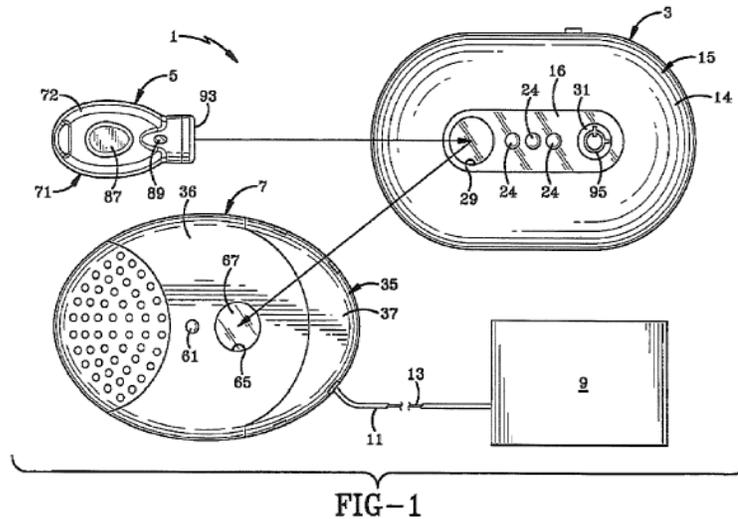


Figure 1 depicts the components of security system 1. *Id.* at 5:15–16. The primary components of security system 1 are programming station 3, programmable key 5, and alarm module 7. *Id.* at 6:18–21. Merchandise 9 is connected to alarm module 7 via cable 11 that preferably contains sense loop 13. *Id.* at 6:21–23. Programming station 3 “includes a housing 15 formed by an internal housing shell 16 preferably having at least a portion

thereof formed of an infrared clear plastic material to facilitate the transfer of infrared wireless communication waves.” *Id.* at 6:29–34.

In the disclosed method, programming station 3 is placed in an “on” position. *Id.* at 9:18–20. “Programmable key 5 is placed in key receiving port 29 and activation switch 85 is actuated . . . caus[ing] logic control circuit 18 of programming station 3 to randomly generate a unique security code (i.e. SDC)” *Id.* at 9:21–26. The SDC is transmitted via communication circuit 20 to programmable key 5, where it is stored in memory 81. *Id.* at 9:26–29. Once programmed with the SDC, programmable key 5 is taken to one or more alarm modules 7 (or other security devices) and inserted into key receiving port 65. *Id.* at 9:43–46. The key then programs the SDC into the memory of alarm module 7. *Id.* at 9:47–53.

D. Illustrative Claim

Petitioner challenges claims 1–10 and 12–45 of the ’472 patent, of which claims 1, 17, and 39 are independent. Claim 1 is illustrative of the challenged claims and is reproduced below:

1. A method for protecting items of merchandise from theft, the method comprising:
providing a single security code with a programming station, the single security code usable in only a single retail store;
inserting an end of the programmable key within a port defined in a housing of the programming station;
storing the single security code at the programmable key; and
storing the single security code at a security device, the security device comprising an alarm and a memory for storing the single security code, the security device configured to be attached to an item of merchandise, the security device further configured to activate the alarm in response to the integrity of the security device being compromised,

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.