Trials@uspto.gov
571-272-7822

Paper 41
Entered: May 24, 2018

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MOBILE TECH, INC.,
Petitioner,

v.

INVUE SECURITY PRODUCTS INC.,
Patent Owner.

Cases IPR2017-00344 and IPR2017-00345
Patent 9,396,631 B2

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

GALLIGAN, *Administrative Patent Judge*.

FINAL WRITTEN DECISION
35 U.S.C. § 318(a)

I. BACKGROUND

Petitioner Mobile Tech, Inc. filed two Petitions requesting *inter partes* review of claims 1–29 of U.S. Patent No. 9,396,631 B2 (Ex. 1001,[1] "the '631 patent") in Cases IPR2017-00344 and IPR2017-00345. On May 26, 2017, we instituted trial in IPR2017-00344 on claims 1–13, 15–19, and 21–29, and we instituted trial in IPR2017-00345 on claims 1–29. In each proceeding, Patent Owner InVue Security Products Inc. filed a Patent Owner Response and Petitioner filed a Reply, as listed in the following chart.

Case Number	Claims Instituted	Decision on Institution	Petition	Response	Reply
IPR2017-00344	1–13, 15–19, and 21–29	Paper 7 ("-344 Dec. on Inst.")	Paper 1 ("-344 Pet.")	Paper 13 ("-344 PO Resp.")	Paper 15 ("-344 Reply")
IPR2017-00345	1–29	Paper 7 ("-345 Dec. on Inst.")	Paper 1 ("-345 Pet.")	Paper 11 ("-345 PO Resp.")	Paper 12 ("-345 Reply")

In each proceeding, we also granted in part Patent Owner's requests for limited discovery related to Petitioner's identification of real parties-in-interest and authorized Patent Owner to file a motion to terminate. -344 Paper 20; -345 Paper 17. Patent Owner filed a motion to terminate in each proceeding, Petitioner filed an opposition to each motion, and we denied the motion in each proceeding, as listed in the following chart.

[1] The '631 patent is Exhibit 1001 in each proceeding. Citations may be preceded by "-344" to designate IPR2017-00344 or "-345" to designate IPR2017-00345.

Case Number	Motion	Opposition	Denial of Motion
IPR2017-00344	Paper 27 (non-public), Paper 33 (public)	Paper 28 (non-public), Paper 30 (public)	Paper 34 (non-public), Paper 37 (public)
IPR2017-00345	Paper 24 (non-public), Paper 32 (public)	Paper 25 (non-public), Paper 27 (public)	Paper 30 (non-public), Paper 34 (public)

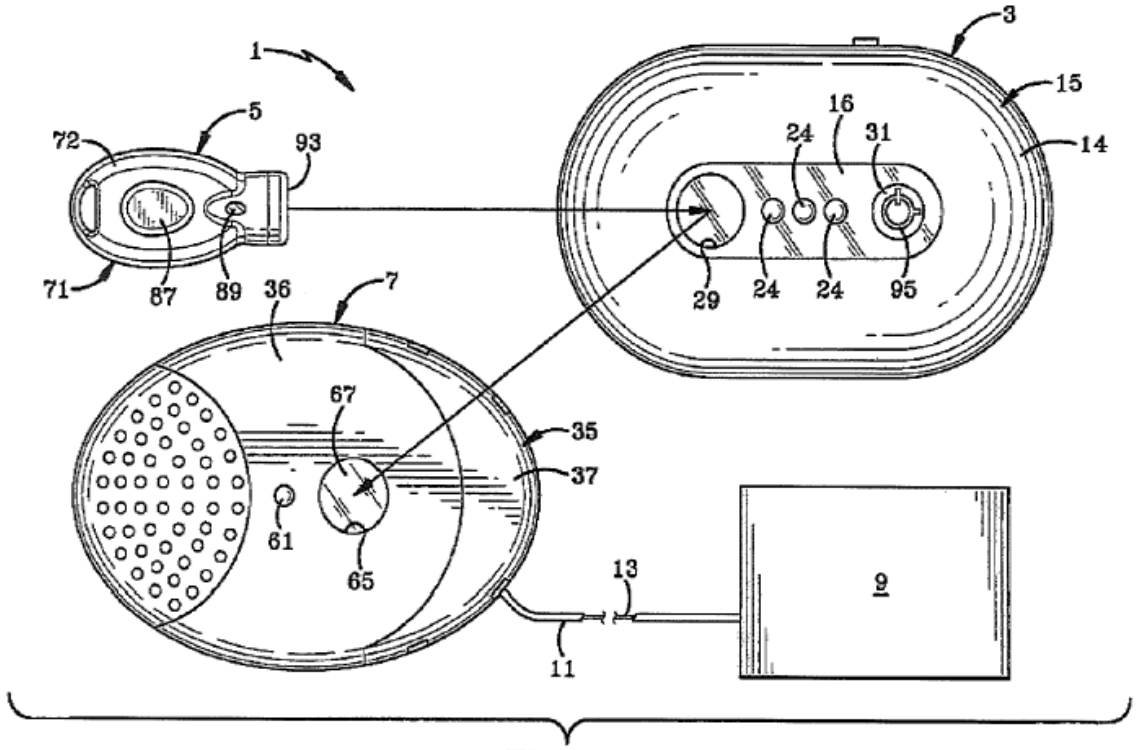
In addition, in IPR2017-00344 the parties filed a Joint Motion to Limit the Petition by removing the ground of unpatentability based on U.S. Patent Application Publication 2007/0159328 A1 (-344 Ex. 1002, published July 12, 2007, "Belden"). -344 Paper 39. We consolidated the two proceedings pursuant to 35 U.S.C. § 315(d) and granted the parties' Motion. -344 Paper 40. As a result, Petitioner's asserted ground challenging claims 1–29 as unpatentable under 35 U.S.C. § 102(b) over Belden is no longer at issue in this proceeding.

An oral hearing was held for both proceedings on January 31, 2018, and a transcript of the hearing is included in the record of each proceeding (-344 Paper 25, "Tr."; -345 Paper 22).

We have jurisdiction under 35 U.S.C. § 6. This Decision is issued pursuant to 35 U.S.C. § 318(a). For the reasons that follow, we determine that Petitioner has shown, by a preponderance of the evidence, that claims 1–29 of the '631 patent are unpatentable. *See* 35 U.S.C. § 316(e) ("In an inter partes review instituted under this chapter, the petitioner shall have the burden of proving a proposition of unpatentability by a preponderance of the evidence.").

A. The '631 Patent

The '631 patent describes a "programmable security system and method for protecting an item of merchandise." Ex. 1001, Abstract. Figure 1 of the '631 patent is reproduced below.



FIG–1

Figure 1 depicts security system 1 that includes programming station 3, programmable key 5, and alarm module 7 adapted to be attached to item of merchandise 9 by cable 11 with sense loop 13. Ex. 1001, 6:7–13. Programming station 3 randomly generates a unique security code (Security Disarm Code, or "SDC") that is transmitted via a wireless (e.g., infrared) link to programmable key 5, which in turn stores the SDC in key memory. *Id.* at 6:32–34, 7:29–34, 9:11–17. Once programmed with an SDC, programmable key 5 is taken to one or more alarm modules 7 and the SDC

is communicated via circuitry to the respective alarm module, which stores the SDC in its memory. *Id.* at 9:30–39.

Cable 11 extends between alarm module 7 and item of merchandise 9. Ex. 1001, 7:58–60. If sense loop 13 (which contains electrical or fiber optic conductors) is compromised, such as by cutting cable 11 or by pulling the cable loose from alarm module 7 or item of merchandise 9, the alarm module emits an audible alarm. *Id.* at 7:56–8:1. To disarm alarm module 7, programmable key 5 is programmed with a valid SDC and circuits in the alarm module and the key communicate with one another to deactivate the alarm, thereby enabling cable 11 to be removed from the merchandise item. *Id.* at 10:51–63. Programmable key 5 then may be used to re-arm the alarm module. *Id.* at 10:63–67. "[T]o disarm and re-arm alarm module 7, the SDC memory 53 of the alarm module must read the same SDC that was randomly generated by the programming station 3 and programmed into the programmable key 5 and subsequently provided by the key to the alarm module." *Id.* at col. 11:4–8.

B. Illustrative Claim

Claims 1 and 22 are independent. Claim 1 recites:

> 1. A programmable security system for protecting items of merchandise from theft, the programmable security system comprising:
>
> a logic control circuit configured to provide a unique security code, the unique security code being unique to the logic control circuit;
>
> a programmable key comprising a memory configured to store the unique security code; and
>
> a security device comprising an alarm and a memory for storing the unique 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,
>
> wherein the programmable key is configured to control the security device upon a matching of the unique security code stored in the memory of the security device with the unique security code stored by the programmable key.

C. References

The grounds of unpatentability in the instant *inter partes* reviews are based on the following references:

Rothbaum	US 5,543,782	Aug. 6, 1996	-345 Ex. 1003
Ott	US 6,380,855 B1	Apr. 30, 2002	-345 Ex. 1004
Denison	US 2004/0201449 A1	Oct. 14, 2004	-345 Ex. 1002
Roatis	US 2005/0165806 A1	July 28, 2005	-345 Ex. 1005
Burri	EP 0745747 A1	Dec. 4, 1996	-344 Ex. 1006
Uchida	JP 1997-259368	Oct. 3, 1997	-344 Ex. 1003[2]
Garner	CA 2465692 A1	Nov. 2, 2004	-344 Ex. 1005

[2] In this Decision, references to Uchida are to the English translation provided as -344 Exhibit 1004.

D. Grounds of Unpatentability

The instant *inter partes* reviews involve the following grounds of unpatentability.

Reference(s)	**Basis**	**Claim(s) Challenged**
Rothbaum and Denison	§ 103(a)[3]	1–5, 8–27, and 29
Rothbaum, Denison, and Ott	§ 103(a)	6 and 7
Rothbaum, Denison, and Roatis	§ 103(a)	28
Uchida	§ 102(b)	1–5, 8–11, 13, 15, 16, 18, 19, 21–23, and 25–29
Uchida and Garner	§ 103(a)	6 and 7
Uchida and Burri	§ 103(a)	12
Uchida	§ 103(a)	17 and 24

II. ANALYSIS

A. Claim Interpretation

The Board interprets claims in an unexpired patent using the "broadest reasonable construction in light of the specification of the patent in which [they] appear[]." 37 C.F.R. § 42.100(b). Under this standard, we interpret claim terms using "the broadest reasonable meaning of the words in their ordinary usage as they would be understood by one of ordinary skill in the art, taking into account whatever enlightenment by way of definitions or otherwise that may be afforded by the written description contained in the applicant's specification." *In re Morris*, 127 F.3d 1048, 1054 (Fed. Cir. 1997). We presume that claim terms have their ordinary and customary

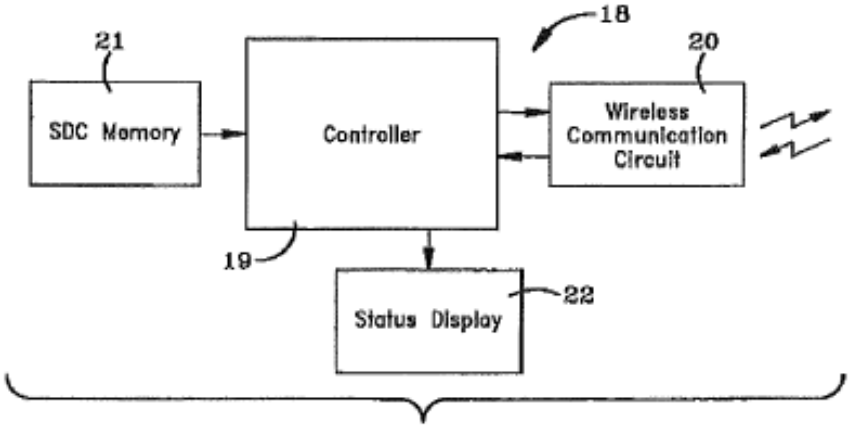
[3] The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) ("AIA"), amended 35 U.S.C. §§ 102, 103, and 112. Because the '631 patent has an effective filing date before the effective date of the applicable AIA amendments, we refer to the pre-AIA versions of 35 U.S.C. §§ 102, 103, and 112.

meaning. *See Trivascular, Inc. v. Samuels*, 812 F.3d 1056, 1062 (Fed. Cir. 2016) ("Under a broadest reasonable interpretation, words of the claim must be given their plain meaning, unless such meaning is inconsistent with the specification and prosecution history."); *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007) ("The ordinary and customary meaning is the meaning that the term would have to a person of ordinary skill in the art in question." (internal quotation marks omitted)). A patentee, however, may rebut this presumption by acting as his own lexicographer, providing a definition of the term in the specification with "reasonable clarity, deliberateness, and precision." *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994).

1. "Logic Control Circuit"

Petitioner contends "a 'collection of computer components' that perform the functionality recited in the claims" is within the broadest reasonable interpretation of the claimed "logic control circuit." -344 Pet. 12 (citing Ex. 1001, 6:27–39, Fig. 4). Patent Owner asserts that Petitioner's proposed interpretation is too broad because it "omits the term 'circuit' from the phrase." -344 PO Resp. 4. Patent Owner argues that "[t]he term 'logic control circuit' is well understood in the art and needs no construction." -344 PO Resp. 4. In its Reply, Petitioner cites the testimony of its declarant, Thaine H. Allison III, that "a person of ordinary skill in the art would understand that those collection of components would necessarily need to be connected through a circuit, so I believe 'circuit' is included in my definition." -344 Ex. 2015, 20:21–25, *quoted in* -344 Reply 2.

Figure 4 of the '631 patent is reproduced below.



FIG–4

Figure 4 depicts logic control circuit 18, which includes main controller 19, security code memory 21, wireless communication circuit 20, and status display 22 having LEDs 24 (shown in Figure 3). Ex. 1001, 6:27–39. The '631 patent states:

> The particular circuitry of logic control circuit 18 is shown in further detail in the U.S. Pat. No. 7,737,844 referenced above, but could be other types of circuitry than that shown therein that are readily known to those skilled in the art for obtaining the features and results of the programming station 3, as discussed further below.

Ex. 1001, 6:62–67. U.S. Patent No. 7,737,844 B2 ("the '844 patent") was at issue in Case IPR2016-01915. During oral argument in that proceeding, Patent Owner agreed that components "connected through a circuit" would be within the scope of a "logic control circuit" as recited in the claims of the '844 patent. IPR2016-01915, Paper 20, 23:4–16.

Based on the foregoing, we are persuaded that "a collection of computer components that are connected through a circuit" is consistent with the language of the claims themselves and the Specification of the '631 patent and, thus, within the broadest reasonable interpretation of "logic

control circuit." We determine that the phrase "logic control circuit" does not require further construction.

2. "Unique Security Code Being Unique to the Logic Control Circuit"

Petitioner argues that the term "unique security code" encompasses codes that are generated in various ways described in the '631 patent. -344 Pet. 12–13 (citing Ex. 1001, 2:29–31, 9:5–22, 13:59–64, 15:24–33). Patent Owner does not dispute Petitioner's particular contentions as to what is within the scope of "unique security code," but argues that the claims also require the code to be "unique to the logic control circuit." -344 PO Resp. 5. Patent Owner argues the term "unique security code" does not require an express construction. -344 PO Resp. 5. We agree with Patent Owner that the claims expressly recite that the code must be "unique to the logic control circuit," and we also determine that the phrase "the unique security code being unique to the logic control circuit" does not require further construction to determine whether the asserted prior art references describe this subject matter.

3. "Configured to Provide a Unique Security Code" (Claim 1); "Providing a Unique Security Code" (Claim 22)

In the Decision on Institution in IPR2017-00344, we determined that "provid[ing] a unique security code" is not limited to "communicating a unique security code to a programmable key using wireless or non-wireless forms of communication," and we also determined that no further construction was necessary. -344 Dec. on Inst. 6. In its Response, Patent Owner argues "that the terms *providing* and *configured to provide* are irrelevant to communication between devices." -344 PO Resp. 6. During oral argument, however, Patent Owner acknowledged that if something is

supplying a code or otherwise communicating it, then the code is being provided and, therefore, that providing is not irrelevant to communication. Tr. 42:7–11. Consistent with our Decision on Institution, we determine that providing a code encompasses communicating the code, although it is not limited to "how the logical control circuit provides the security code to the key," as Petitioner asserts. *See* -344 Pet. 13. "Rather, claims 1 and 22 recite 'provid[ing] a unique security code,' without reciting that the 'programmable key' is the device to which it is provided." -344 Dec. on Inst. 5–6. Indeed, claim 27 includes a further limitation to claim 22 of "communicating the unique security code to the programmable key."

We determine that no further construction of the "providing" limitations is necessary.

4. Remaining Terms

We determine that the remaining terms of the claims do not require express construction.

B. Principles of Law

To establish anticipation, each and every element in a claim, arranged as recited in the claim, must be found in a single prior art reference. *Net MoneyIN, Inc. v. VeriSign, Inc*., 545 F.3d 1359, 1371 (Fed. Cir. 2008). Although the elements must be arranged or combined in the same way as in the claim, "the reference need not satisfy an *ipsissimis verbis* test," i.e., identity of terminology is not required. *In re Gleave*, 560 F.3d 1331, 1334 (Fed. Cir. 2009).

A patent claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter 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. *KSR Int'l Co. v. Teleflex Inc*., 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) any secondary considerations, if in evidence.[4] *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

C. Level of Ordinary Skill in the Art

Petitioner's declarant, Mr. Allison, testifies that a person of ordinary skill in the art

> would have had a four year technical degree (*e.g.* B.S. engineering) with a minimum of three years of experience in using, provisioning, designing or creating, or supervising the design or creation, of such theft prevention devices, and other related security devices. Extended experience in the industry could substitute for a technical degree. A [person of ordinary skill in the art] would have known how to research the technical literature in fields relating to theft prevention, including in retail and other environments, as well as security in general. Also, a [person of ordinary skill in the art] may have worked as part of a multidisciplinary team and drawn upon not only his or her own skills, but also taken advantage of certain specialized skills of others in the team, *e.g.*, to solve a given problem. For example, designers, engineers (*e.g.*, mechanical or electrical), and computer scientists or other computer programmers may have been part of a team.

-344 Ex. 1017 ¶ 22; -345 Ex. 1010 ¶ 19. Patent Owner provides a slightly different skill level:

[4] Patent Owner does not present arguments or evidence of such secondary considerations.

> [A person of ordinary skill in the art] would have the equivalent of a four-year degree in electrical engineering, computer engineering, computer science, or the equivalent and would also have approximately two to five years of professional experience and be trained in electronics including microcontrollers, and embedded programming for microcontrollers.

-344 PO Resp. 6–7 (citing Ex. 2006[5] ¶¶ 32–34); -345 PO Resp. 7.

Neither party explains in detail why its proposed level of ordinary skill in the art should be adopted nor how the different levels affect the parties' analyses. Although there are slight differences between the proposed levels of ordinary skill in the art, the parties' declarants agree that an ordinarily skilled artisan would have had a four-year technical degree or the equivalent and some amount of professional experience. Based on the evidence of record, the subject matter at issue, and the prior art of record, we determine that a person of ordinary skill in the art would have had a four-year technical degree or equivalent experience with a minimum of two years of professional technical experience in the field of theft prevention devices or related security devices. We apply this level of ordinary skill in the art for purposes of this Decision.

D. Unpatentability Challenge Based on Rothbaum and Denison (§ 103(a) – Claims 1–5, 8–27, and 29)

Petitioner contends that claims 1–5, 8–27, and 29 would have been obvious based on the combination of Rothbaum and Denison. -345 Pet. 7, 14–51. Petitioner explains how the cited prior art references teach the claimed subject matter, provides reasoning as to why one of ordinary skill in

[5] Exhibit 2006 is the Declaration of Harry Direen, Ph.D., P.E., which Patent Owner submitted with its preliminary responses in the following cases involving patents related to the '631 patent: IPR2016-00892, -895, -896, -898, and -899.

the art would have been motivated to combine their respective teachings, and relies upon the testimony of Mr. Allison to support its positions. *Id.* at 14–51.

1. Overview of Rothbaum

Rothbaum is directed to an electronic security system for monitoring merchandise that provides for the sounding of an alarm based on an indication from a sensor. -345 Ex. 1003, Abstract. The system is intended to be used for theft prevention in retail stores, hotels, and other businesses. *Id.* at 1:6–9. Figure 1 of Rothbaum is reproduced below.

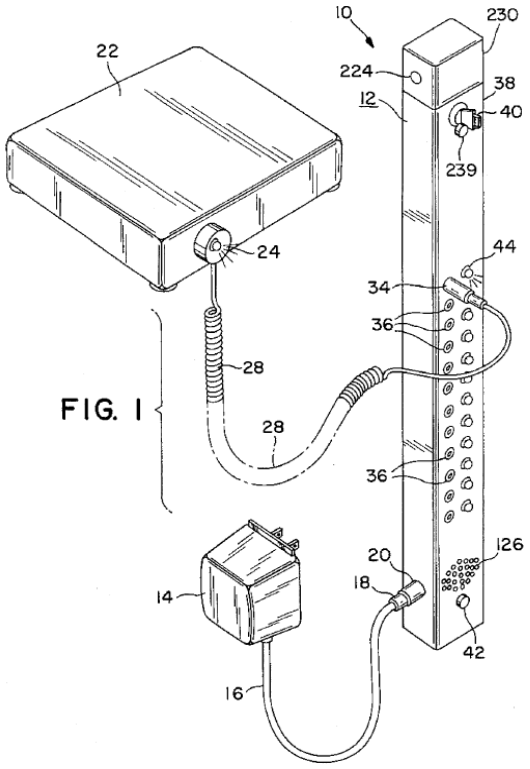


Figure 1 depicts a perspective view of Rothbaum's security system. *Id.* at 4:22–23. Article 22 is the merchandise being protected by security system 10. *Id.* at 5:5–9, 5:49–50. Sensor 24 is attached to article 22. *Id.* at 5:54–56, 5:62–64. Item cord 28 connects sensor 24 to the alarm circuitry

located in housing 12. *Id.* at 5:16–17, 6:1–2. An alarm will sound and an LED will light when an alarm condition occurs. *Id.* at 3:43–47.

2. Overview of Denison

Denison discloses vending machines equipped with programmable electronic locks. -345 Ex. 1002 ¶ 2. As used in Denison, a "vending machine" is "a device that performs a money transaction, which may involve the insertion of cash or commercial paper, or the swiping of a credit and/or debit card, and may (but [is] not required to) dispense an item or items or provide functions in response to the money transaction," and broadly covers "machines commonly used for vending drinks and snacks, ATM stations, change machines, toll machines, coin-operated laundry machines, video arcades, etc." *Id.* ¶ 36. Access to the contents of the disclosed vending machine is controlled by an electronic lock and electronic key. *Id.* ¶ 7. To unlock the electronic lock and open the vending machine, there must be a match between the code stored in the electronic key and the code stored in the electronic lock. *Id.* ¶ 42. Figure 1 of Denison is reproduced below.

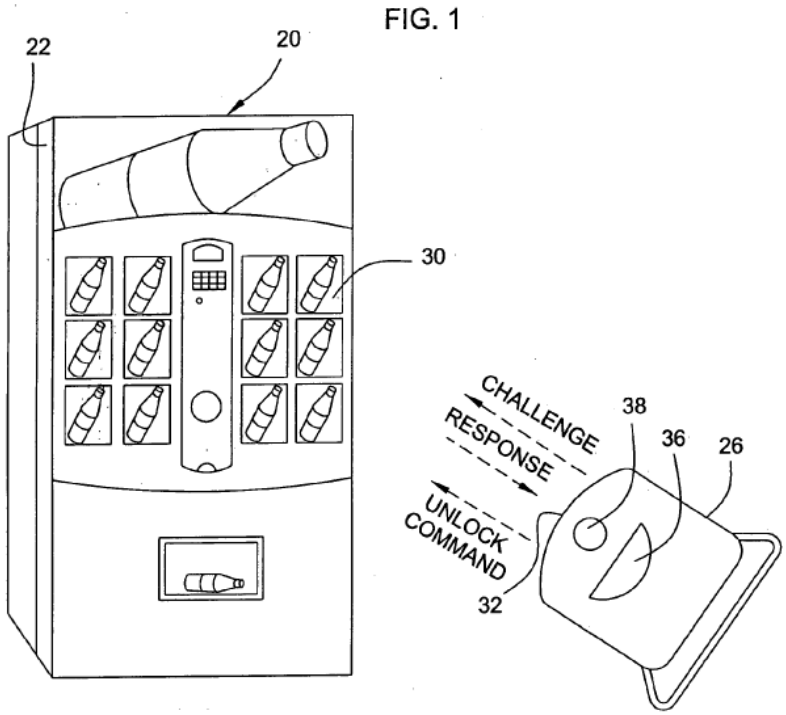


Figure 1 is a schematic view of Denison's vending machine and electronic lock. *Id.* ¶¶ 15, 36–37. Vending machine 20 has front panel or door 22 that can be opened when the electronic lock is wirelessly unlocked using properly programmed electronic key 26. *Id.* ¶¶ 36–37.

Figure 17 of Denison is reproduced below.

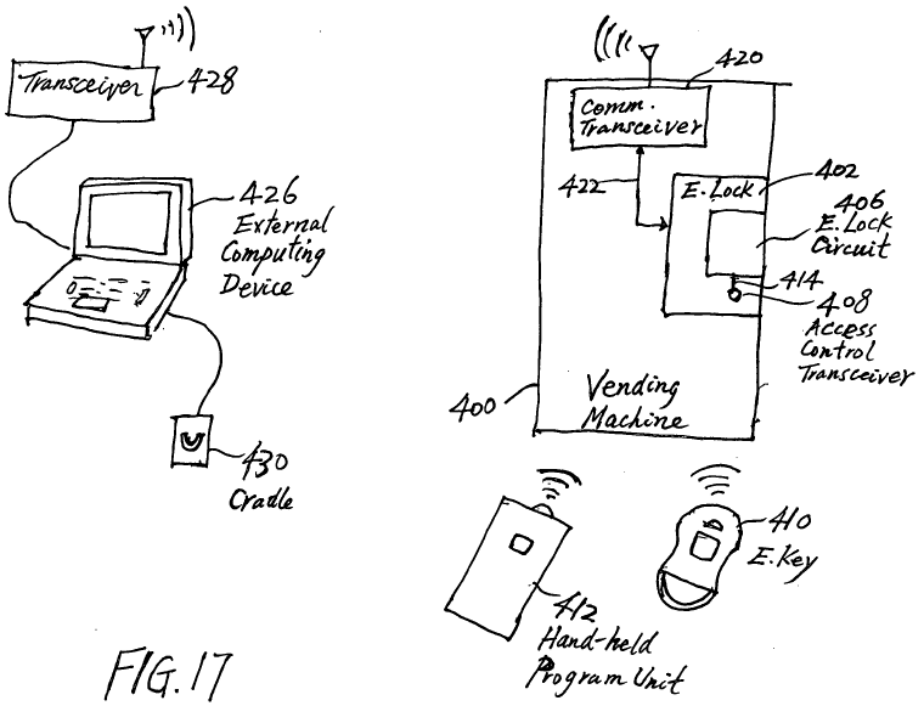


FIG. 17

Figure 17 depicts external computing device 426 (e.g., a laptop computer) with wireless transceiver 428 and cradle 430, electronic key 410, and vending machine 400 with wireless transceiver 420 and electronic lock 402 having microprocessor-based electronic lock circuit 406 and wireless transceiver 408. -345 Ex. 1002 ¶¶ 31, 77–78. External computing device 426 may be used to generate a new "access code" and wirelessly program it into the electronic lock "without having to open the vending machine to access a program switch" and also to program the access code into the electronic key. *Id.* ¶¶ 77–79, 83–85. Denison discloses that

> the external computing device 426 may optionally be used to program an electronic key 410 that can be used to visit and access the vending machine 400 through the access control transceiver 408. To that end, the electronic key 410 is connected to the cradle 430, and the access code that has been programmed into the lock is transmitted via the cradle into the

> key, together with any other appropriate access control parameters for the key. The key 410 can then be used to access the vending machine by communicating with the electronic lock circuit 406 via the access control transceiver 406 based on the newly programmed access code(s) and control parameters.

Id. ¶ 85.

3. Whether Rothbaum and Denison are Analogous Art

As an initial matter, to be considered for obviousness, a reference must be analogous art. *See In re Bigio*, 381 F.3d 1320, 1325 (Fed. Cir. 2004) ("References within the statutory terms of 35 U.S.C. § 102 qualify as prior art for an obviousness determination only when analogous to the claimed invention."). A prior art reference qualifies as analogous art (1) if it is from the same field of endeavor as the claimed invention, regardless of the problem addressed, or (2) if the reference is not within the field of the inventor's endeavor, it is nonetheless reasonably pertinent to the particular problem with which the inventor is involved. *Id.*

Petitioner argues that "Denison and Rothbaum are in the field of security devices for the protection of merchandise." -345 Pet. 17 (citing -345 Ex. 1010 ¶¶ 78–79). The '631 patent describes the "Field of the Invention" as follows:

> The invention relates to security systems and methods for protecting merchandise from theft, and in particular, to a security system and method including a programmable key that is programmed with a security code from a programming station and is subsequently used to program and/or operate an alarm module attached to an item of merchandise.

Ex. 1001, 1:26–31. Therefore, the '631 patent itself describes the relevant field of endeavor as "protecting merchandise from theft." Further, claims 1

and 22 are directed to a programmable security system and a method "for protecting items of merchandise from theft."

We find that Rothbaum and Denison are analogous to the claimed invention because both references are in the same field of endeavor as the claimed invention, namely protecting merchandise from theft. In particular, Rothbaum is directed to "security systems, and more specifically to electronic security systems used in retail stores, offices, hotels and other establishments to prevent the theft of merchandise." -345 Ex. 1003, 1:6–9.[6] Similarly, Denison's disclosure of electronically-locking vending machines is directed to protecting merchandise from theft. *See* -345 Ex. 1002 ¶ 9 ("The use of the field-programmable electronic locks for vending machines provides an effective way to reduce theft and fraud in terms of unauthorized access to the machines.").[7] Therefore, both references qualify as analogous prior art to the challenged claims.

---

[6] During the oral argument for several cases involving patents related to the '631 patent, counsel for Patent Owner acknowledged that Rothbaum is analogous art to U.S. Patent No. 9,269,247 B2, of which the '631 patent is a continuation. IPR2016-00899, Paper 29, 94:21–22.

[7] In its Response, Patent Owner argues that "[v]ending machines are not analogous to retail merchandise systems (using alarms) as [Petitioner] alleges." -345 PO Resp. 10. Patent Owner made the same argument in several cases involving patents related to the '631 patent. *E.g.*, IPR2016-00895, Paper 18, 34; IPR2016-00899, Paper 16, 31. During the oral argument for these cases, counsel for Patent Owner stated that "Denison is only somewhat analogous to retail store security" and later clarified that Patent Owner's argument in those cases was that Petitioner has not set forth a sufficient rationale to combine the teachings of Rothbaum and Denison, not that Denison is not analogous art to the patents at issue. IPR2016-00899, Paper 29, 95:11–97:2.

4. Independent Claims 1 and 22

Petitioner relies on Rothbaum for teaching certain limitations of claims 1 and 22 and relies on Denison for teaching other limitations. *See* -345 Pet. 14–35. Below we address the parties' contentions as to each reference and then address their arguments with respect to the combined teachings of Rothbaum and Denison.

a. Claim limitations taught by Rothbaum

Claim 1 is directed to "[a] programmable security system for protecting items of merchandise from theft," and independent claim 22 is directed to "[a] method for protecting items of merchandise from theft." Petitioner contends Rothbaum discloses a security system for protecting merchandise, as illustrated in Figure 1, discussed above. -345 Pet. 14–15, 20.

We are persuaded by Petitioner's argument, and we find Rothbaum discloses a security system for protecting items of merchandise from theft and a method for protecting items of merchandise from theft. For example, in Figure 1 of Rothbaum, "a twelve jack security system 10 is shown which can protect twelve items of merchandise." -345 Ex. 1003, 5:10–11; *see also id.* at 1:6–9 ("The present invention generally relates to security systems, and more specifically to electronic security systems used in retail stores, offices, hotels and other establishments to prevent the theft of merchandise.").

Petitioner argues Rothbaum's disclosure of "strip or housing 12" connecting to article of merchandise 22 via "item cord 28" teaches a "security device configured to be attached to an item of merchandise," as recited in independent claim 1, and "a security device attached to an item of

merchandise," as recited in independent claim 22. -345 Pet. 15, 25–27, 34 (citing, *inter alia*, -345 Ex. 1003, Fig. 1, 5:62–6:4). We are persuaded by Petitioner's argument, and we find Rothbaum teaches these limitations of claims 1 and 22 based on Rothbaum's disclosure in Figure 1 that item cord 28 connects strip 12 to sensor 24 on article of merchandise 22. *See* Ex. -345 1003, 5:62–6:2 ("Hard goods sensor 24, including a sensor housing 23, is attached to the article 22 . . . . Item cord 28 is of sufficient length to connect the sensor 24 to the alarm circuitry in strip 12."); *see also* -345 Ex. 1010 ¶ 67.

Petitioner also argues Rothbaum discloses that its security device has an "alarm" (horn 126) and that Rothbaum teaches that the security device is "configured to activate the alarm in response to the integrity of the security device being compromised," as recited in independent claim 1, and that "the security device compris[es] an alarm configured to be activated in response to the integrity of the security device being compromised," as recited in claim 22. -345 Pet. 15, 26–27, 34 (citing, *inter alia*, -345 Ex. 1003, 6:15–22, 8:22–28, 12:10–18, Fig. 1). We are persuaded by Petitioner's argument, and we find Rothbaum teaches this subject matter based on the following disclosure of Rothbaum:

> As can be seen in FIG. 12, tamper switch 225 is normally open. The tamper switch is activated by the battery compartment screw 224 as can be seen in FIG. 1. If an unauthorized person attempts to tamper with the battery 226, by opening the battery compartment cover 220, they must loosen screw 224. As screw 224 is removed, tension on the activator of switch 225 is moved thus closing switch 225. When switch 225 closes, transistor 122 is turned on thus activating horn 126.

-345 Ex. 1003, 12:10–18. We find that the integrity of the security device is compromised when the battery compartment is opened. *See* -345 Ex. 1010, 37.

Petitioner further argues Rothbaum teaches a key for controlling the security device by disarming the security device after a security breach occurs. -345 Pet. 15 (citing -345 Ex. 1003, 6:15–22, 8:22–28). We are persuaded by Petitioner's argument, and we find Rothbaum teaches a key for disarming the security device after a breach occurs because Rothbaum discloses that, "once a breach of security condition is detected, the alarm horn 126 will sound [u]ntil key switch 38 is turned from the ON position to the SET position." -345 Ex. 1003, 8:23–25.

Petitioner notes Rothbaum does not disclose a programmable key and, instead, relies on Denison to teach a programmable key and a logic control circuit. -345 Pet. 15–16.

b. Claim limitations taught by Denison

As discussed above, Denison discloses vending machines having electronic locks that can be controlled with electronic keys programmed by an external computing device. -345 Ex. 1002, Abstract, ¶¶ 2, 6, 85, Figs. 1 and 17. Petitioner relies on Denison's disclosures for various limitations of claims 1 and 22 as explained below.

i. Logic control circuit

Petitioner argues that internal components of Denison's external computing device constitute "a logic control circuit configured to provide a unique security code, the unique security code being unique to the logic control circuit," as recited in claim 1, and the similarly recited "logic control

circuit" of claim 22. -345 Pet. 20–23, 34 (citing -345 Ex. 1002 ¶¶ 43, 78, 84, 85, Figs. 17, 21; -345 Ex. 1010, 31–34). In particular, Petitioner contends that Denison discloses that its external computing device generates an "access code" and transmits it to an electronic key. -345 Pet. 20–23 (citing -345 Ex. 1002 ¶¶ 43, 78, 84, 85, Figs. 17, 21). Petitioner further contends that a person of ordinary skill in the art would have understood that internal components of the external computing device, such as a microprocessor, random-access memory (RAM), and communication interfaces and circuits, perform the access code generation and transmission and, therefore, teach a "logic control circuit." -345 Pet. 21–23 (citing -345 Ex. 1010, 31–34).

Patent Owner argues that Petitioner "fails to specifically identify the *logic control circuit* within Denison (or any other reference)." -345 PO Resp. 17. Patent Owner acknowledges that "Denison may contain a collection of computer components" but contends that Petitioner has not shown how the alleged collection "forms a 'circuit' for controlling the logic of the apparatus." *Id.* We disagree. As explained above, we interpret "logic control circuit" as encompassing a collection of computer components that are connected through a circuit. *See supra* Section II.A.1. Denison discloses: "[T]he external computing device 426 may also have programs that implement[] mathematical algorithms for computing the access codes and control parameters. Such calculations may generate the access codes randomly or based on a function that includes the time as a variable." -345 Ex. 1002 ¶ 84. Denison also discloses external computing device 426 may be "a laptop computer." *Id.* ¶ 78. We are persuaded by Petitioner's argument, supported by the testimony of Mr. Allison, that "a [person of

ordinary skill in the art] would understand that in order to randomly generate a number, the external computing device, which is a laptop, would have to use its internal components, such a microprocessor and/or RAM." -345 Pet. 22 (citing -345 Ex. 1010, 32–33). Furthermore, we are persuaded that these internal components are part of a circuit because they electrically communicate with each other; otherwise, the device would not work as described in Denison. *See* -345 Pet. 21–23; -345 Reply 14–15. Thus, we disagree with Patent Owner's argument that Petitioner fails to specify how Denison teaches a "logic control circuit."

Denison discloses an external computing device that computes access codes randomly with each code being one of one million possible values. -345 Ex. 1002 ¶¶ 84 ("Such calculations may generate the access codes randomly or based on a function that includes the time as a variable."), 43 ("In one implementation as shown in FIG. 5A, a key code 68 stored in an electronic key includes seven (7) digits. The first digit of the key code is used to indicate the type of the key. . . . The next 6 digits in the key code are the access code (000,000 to 999,999)."). Denison further discloses that "external computing device 426 may optionally be used to program an electronic key 410" via cradle 430, as depicted in Figure 21. -345 Ex. 1002 ¶ 85. We find Denison's disclosure of a computing device such as a laptop that generates an access code and transmits it to an electronic key teaches "a logic control circuit configured to provide a unique security code," as recited in claim 1 and "providing a unique security code with a logic control circuit," as recited in claim 22. We also find that a code that is randomly generated by the external computing device and is one of one million possibilities, as disclosed by Denison, teaches "the unique security code

being unique to the logic control circuit," as recited in claims 1 and 22. -345 Ex. 1002 ¶¶ 43, 84.

We find, therefore, that Denison teaches "a logic control circuit configured to provide a unique security code, the unique security code being unique to the logic control circuit," as recited in claim 1, and "providing a unique security code with a logic control circuit, the unique security code being unique to the logic control circuit," as recited in claim 22.

ii. Programmable key

Petitioner further contends Denison's disclosure of its "electronic key" storing an access code teaches "a programmable key comprising a memory configured to store the unique security code," as recited in claim 1, and "storing the unique security code at a programmable key," as recited in independent claim 22. -345 Pet. 15–16, 23–25, 34 (citing -345 Ex. 1002 ¶¶ 6, 15, 41–44, 77, 85, 86, Figs. 1, 5B, 17). Petitioner argues Denison "discloses that its 'electronic key' has a memory for storing the 'access code' (*i.e.*, unique security code)." *Id.* at 24 (citing -345 Ex. 1002 ¶¶ 41, 86; -345 Ex. 1010, 35).

We are persuaded by Petitioner's contentions. Denison discloses that "electronic key 26 includes . . . a nonvolatile memory 82," which "is for storing a key code 88." -345 Ex. 1002 ¶ 41; *see also id.* ¶ 42 ("Each electronic key 26 has a key code 88 stored therein . . . ."). As discussed above, Denison discloses that its "key code" is seven digits, of which six are the access code. -345 Ex. 1002 ¶ 43 ("In one implementation as shown in FIG. 5A, a key code 68 stored in an electronic key includes seven (7) digits. The first digit of the key code is used to indicate the type of the key. . . . The

next 6 digits in the key code are the access code (000,000 to 999,999).").

Denison further discloses:

> [T]he external computing device 426 may optionally be used to program an electronic key 410 that can be used to visit and access the vending machine 400 through the access control transceiver 408. To that end, the electronic key 410 is connected to the cradle 430, and the access code that has been programmed into the lock is transmitted via the cradle into the key, together with any other appropriate access control parameters for the key. The key 410 can then be used to access the vending machine by communicating with the electronic lock circuit 406 via the access control transceiver 406 based on the newly programmed access code(s) and control parameters.

-345 Ex. 1002 ¶ 85.

We find, therefore, that Denison teaches "a programmable key comprising a memory configured to store the unique security code," as recited in claim 1, and "storing the unique security code at a programmable key," as recited in claim 22.

iii. Controlling the security device

Petitioner further contends Denison discloses storing the key code, which includes the access code, in the vending machine and unlocking (i.e., controlling) the vending machine using the electronic key if the access codes in the key and the vending machine match. -345 Pet. 16, 27–28 (citing -345 Ex. 1002 ¶ 42; -345 Ex. 1010, 38–39, ¶¶ 72–73). We are persuaded by these arguments.

First, Denison discloses that "[e]ach electronic key 26 has a key code 88 stored therein, and the same key code is stored in the memory 52 of the electronic lock in each vending machine to be operated with the electronic key." -345 Ex. 1002 ¶ 42. Thus, we find Denison discloses "a security

device comprising . . . a memory for storing the unique security code," as recited in claim 1, and "storing the unique security code at a security device," as recited in claim 22.

Second, Denison discloses:

> During each access attempt, the key code in the electronic key is transferred from the key to the electronic lock using a secured communication method. The electronic lock can be unlocked if the key code it receives from the electronic key matches the key code stored in the memory of the lock.

-345 Ex. 1002 ¶ 42. Thus, Denison discloses unlocking the device if the codes in the key and the device match, thus teaching "control[ling] the security device," as recited in claims 1 and 22.

We find, therefore, that Denison teaches that "the programmable key is configured to control the security device upon a matching of the unique security code stored in the memory of the security device with the unique security code stored by the programmable key," as recited in claim 1, and "controlling the security device upon a matching of the unique security code provided by the logic control circuit with the unique security code stored by the security device," as recited in claim 22.

Based on the foregoing discussions of Rothbaum and Denison, we find that the combined disclosures of these references teach the limitations of independent claims 1 and 22. Next, we address Petitioner's reasons as to why a person of ordinary skill in the art would have combined the teachings of Rothbaum and Denison in support of its assertion that the subject matter of independent claims 1 and 22 would have been obvious.

c. Rationale to combine Rothbaum and Denison and reasonable expectation of success

Petitioner argues that Denison addresses various problems with mechanical locks on vending machines, such as key management and distribution and usage of keys. -345 Pet. 16–17 (citing -345 Ex. 1002 ¶¶ 4–6, 9). For example, Denison discloses:

> One significant problem with conventional vending machines is the difficulties in managing the distribution and usage of the keys to ensure the security of the locks on the vending machines. The process of collecting money from the vending machines scattered at different places is a very manpower-intensive operation that requires many employees to go into the field with numerous mechanical keys for operating the locks on the vending machines. It requires a considerable amount of attention and efforts to manage and track the distribution of the keys to the field workers to keep the keys secure.
>
> Moreover, the mechanical keys and lock cores of vending machines are a point of attack for vandals. The keys can be lost or copied easily, and the stolen or copied keys may then be used by an unauthorized person to access the machines, and it is difficult to discover such misuses and security breaches. Also, a skilled vandal can easily pick or drill-out the lock core tumblers and measure the key cuts of the lock core tumblers to re-produce a like key and compromise the security. In the event a security breach is identified, the mechanical lock cores of the affected vending machines typically have to be manually replaced, which is a time-consuming and very costly process. Furthermore, mechanical keys and locks are devices that cannot be partially limited in operation they operate indefinitely if in use. Also, they do not have the ability to record access operation attempts of their operation.

-345 Ex. 1002 ¶¶ 4–5.

Petitioner argues that these problems identified in Denison "would also have been problems present with the security system disclosed in Rothbaum." -345 Pet. 17 (citing -345 Ex. 1010 ¶¶ 78–79). Petitioner's declarant, Mr. Allison, testifies:

> [T]he problems resolved by Denison would also have been problems present with the security system disclosed in Rothbaum. . . . [T]he security device [in Rothbaum] is used to protect merchandise in the retail environment. In this environment, there are also many employees and thus the need for multiple keys, which can get lost or be stolen and then used by unauthorized individuals.

-345 Ex. 1010 ¶ 78.

Petitioner argues that, to address the known problems with mechanical vending machine locks, Denison discloses the use of electronic, field-programmable keys and locks. -345 Pet. 16–17 (citing -345 Ex. 1002 ¶¶ 9–10, 79). Denison describes the advantages of such electronic locks and keys:

> The use of the field-programmable electronic locks for vending machines provides an effective way to reduce theft and fraud in terms of unauthorized access to the machines. The electronic keys provide a greater level of key security compared to mechanical keys, as they cannot be copied as easily as conventional mechanical keys. The use of non-contact wireless data communication between the key and the lock prevents breeches of security associated with vandals measuring key cuts, copying keys and picking locks. The use of data encryption in the wireless communications between the key and the lock prevents the key code from being copied by electronic monitoring and eavesdropping. The data transmission between the key and lock may be implemented in the infrared range to provide close-proximity highly directional communication of secure codes to further prevent eavesdropping of the security codes and to prevent accidental unlocking of locks.

> The use of programmable electronic locks on vending machines and the associated electronic keys also provides advantages in terms of significant reduction in the costs associated with managing the distribution of the keys for unlocking the machines and the monitoring of the usage of the keys. Key IDs in addition to the key codes used in accessing the lock may be used to distinguish keys having the same key codes. Customized access limitations may be programmed by a supervisor into the electronic keys to restrict when and how they can be used to access the vending machines. Each key may also be programmed with a specific list of lock IDs identifying the electronic locks on vending machines that the key is allowed to unlock.

-345 Ex. 1002 ¶¶ 9–10.

Petitioner contends a person of ordinary skill in the art "would have therefore been motivated to combine the teachings of Denison with Rothbaum to move from a mechanical key system to an electronic key system to achieve the advantages identified by Denison." -345 Pet. 17 (citing -345 Ex. 1010 ¶¶ 78–79). Petitioner further contends a person of ordinary skill in the art would have

> fully understood how to create and use security devices with electronic keys well before the time of the alleged invention. In connection with the Rothbaum security system, a [person of ordinary skill in the art] thus would have had a reasonable expectation of success in progressing from the Rothbaum mechanical key system to a programmable key system like that of Denison.

Id. at 18–19 (citing -345 Ex. 1010 ¶¶ 83–84).

Patent Owner makes several arguments as to why Petitioner allegedly does not provide sufficient reasoning to justify the combination of Rothbaum and Denison, and in support it cites the testimony of Mr. Fawcett,

a named inventor on the '631 patent. -345 PO Resp. 8–16 (citing Ex. 2010[8] ¶¶ 62, 64–68, 70). For instance, Patent Owner disputes Petitioner's assertion that the "problems resolved by Denison would also have been problems present with the security system disclosed in Rothbaum." *Id.* at 12 (quoting -345 Pet. 17). Patent Owner argues:

> Nothing in Rothbaum . . . teaches or suggests that its mechanical key has any problems. *See* Ex. 2009, 227:23–228:1. Rothbaum's disclosure of a key is very straightforward, generally focusing on the basic functionality of the mechanical key. Ex. 1003 at 6:17–22. At no point does Rothbaum mention problems with such mechanical keys, nor does it explicitly or implicitly suggest the mechanical key needs replacing or improvement. Ex. 2010 ¶ 65.

-345 PO Resp. 12. Mr. Fawcett testifies similarly, citing column 6, lines 17–22 of Rothbaum in his testimony. *See* Ex. -345 2010 ¶ 65.[9]

Although we agree with Patent Owner that Rothbaum does not expressly disclose problems with its own key, Petitioner's contentions of obviousness are not premised on any such disclosure in Rothbaum. Rather, Petitioner contends, and Mr. Allison testifies, that the problems Denison identifies with respect to mechanical keys also would have been issues in Rothbaum's system, which uses mechanical keys. -345 Pet. 17; -345 Ex. 1010 ¶ 78. Mr. Allison explains that the security device of Rothbaum "is used to protect merchandise in the retail environment" and that, "[i]n this

[8] Exhibit 2010 is the Declaration of Christopher J. Fawcett in Support of Patent Owner's Responses in IPR2016-00895 and IPR2016-00896, both of which involve U.S. Patent No. 9,135,800 B2 ("the '800 patent"). The '631 patent is a continuation of U.S. Patent No. 9,269,247 B2, which in turn is a continuation of the '800 patent.

[9] Although Mr. Fawcett cites column 7, lines 17–22 of Rothbaum, the quoted passage appears at column 6, lines 17–22 of Rothbaum. *See also* -345 PO Resp. 12 (citing -345 Ex. 1003, 6:17–22).

environment, there are also many employees and thus the need for multiple keys, which can get lost or be stolen and then used by unauthorized individuals." -345 Ex. 1010 ¶ 78. Rothbaum itself discloses that "[o]nly authorized personnel should have access to key 40 to prevent the circumvention of the security system" (-345 Ex. 1003, 6:20–22), underscoring the very security issues identified by Mr. Allison that are encountered in a retail environment. *See* -345 Ex. 1010 ¶ 78. Therefore, we credit Mr. Allison's testimony that the problems Denison identifies with respect to mechanical keys also would have been issues in Rothbaum's system. *Id.*

Patent Owner also argues that Rothbaum's concerns with power conservation and device integration undermine Petitioner's rationale to combine. -345 PO Resp. 13–14. With respect to power conservation, Patent Owner argues:

> Rothbaum was also concerned with the need to conserve power in the closed loop system. Ex. 1003, 2:30–35. Denison's external computing device, keys and electronic lock, although working well on a vending machine without the same power concerns, would likely worsen the power drain that Rothbaum conscientiously seeks to minimize or avoid. *Id.* at 2:30–35; Ex. 2010 ¶ 67.

-345 PO Resp. 13. The cited portion of Rothbaum, however, describes a drawback of closed loop security systems when the power is off, such as during a power outage (-345 Ex. 1003, 2:30–35), and Rothbaum discloses the use of "an energy conservation mode" in which a battery supplies power in such circumstances (*id.* at 3:63–4:14). Rothbaum does not appear to have the same concerns with power conservation during normal operation, as it discloses the use of a closed system that is powered by an AC adapter when

power is on. *Id.* at 3:63–64 ("The instant invention is a closed system when drawing power from its AC adapter."). We do not find that Rothbaum's disclosure of the use of an energy conservation mode when power is off undermines Petitioner's asserted rationale to combine. Indeed, Denison's disclosure that external computing device 426 is a laptop computer (-345 Ex. 1002 ¶ 78) complements Rothbaum's energy conservation mode because a laptop computer would have a battery and need not be plugged into an outlet at all times. For example, Denison describes that "an operator may drive to the building in which the vending machine is located. *In his service vehicle*, the operator uses a laptop computer that functions as the external computer device to wirelessly communicate with the electronic lock of the vending machine by sending RF signals." *Id.* ¶ 86 (emphasis added).

Patent Owner argues:

> A [person of ordinary skill in the art] would also not modify Rothbaum to add components that are not integrated. During prosecution of its application, Rothbaum described that the "invention provides a fully integrated security device [which] advantageously enables alarm and detection circuitry and connections to sensors be located within one housing [in] a completely self-contained unit." Ex. 2011, 4. Modifying Rothbaum to include a programming station and programmable key would lead to additional circuitry being outside the housing and a reduction in simplicity and security. Ex. 2010 ¶ 68.

-345 PO Resp. 13 (first alteration added). As we understand Petitioner's contentions, however, the security device of the Rothbaum-Denison combination remains an integrated device having alarm and detection circuitry and sensor connections located within one housing. In particular, as discussed above, Rothbaum's strip or housing 12 is a "security device" as recited in claims 1 and 22. Petitioner does not argue that the programming

station that houses the logic control circuit of the Rothbaum-Denison combination would have alarm and detection circuitry and sensor connections. Therefore, the inclusion of a programming station in the combined Rothbaum-Denison security *system* would not affect the location of these components in the security device itself.

Patent Owner also argues that "Rothbaum, in particular, seems to be concerned with avoiding complexity," and, therefore, "[m]odifying Rothbaum's system (as alleged by [Petitioner]) to supplant a simple mechanical key with Denison's distributed electronic key system would only increase complexity, costs, and the risk of improper installation by adding extensive additional electronic components." -345 PO Resp. 12–13 (citing -345 Ex. 1003, 2:1–6; -345 Ex. 2010 ¶ 66). We do not disagree that adapting Rothbaum's system to include electronic keys as taught by Denison may result in a more complex system, but this alone does not undermine Petitioner's asserted rationale for the combination. As the U.S. Court of Appeals for the Federal Circuit has stated, "a given course of action often has simultaneous advantages and disadvantages, and this does not necessarily obviate motivation to combine." *Medichem, S.A. v. Rolabo, S.L.*, 437 F.3d 1157, 1165 (Fed. Cir. 2006). "Instead, the benefits, both lost and gained, should be weighed against one another." *Id.* (quoting *Winner Int'l Royalty Corp. v. Wang*, 202 F.3d 1340, 1349 n.8 (Fed. Cir. 2000)).

Even if the proposed combination introduces complexities that are not present in the system of Rothbaum alone, we also consider the advantages that electronic keys provide, as described in Denison, such as greater security and improved key management and distribution. *See* -345 Ex. 1002 ¶¶ 9–10. We find such advantages would have outweighed any added

complexity and motivated a person of ordinary skill in the art to adapt Rothbaum's system to use electronic keys. In other words, based on the disclosures of the references, a person of ordinary skill in the art would have considered the use of electronic keys to be a significant *improvement* to the mechanical system of Rothbaum, regardless of the minimal added complexity of such a change.

Further, we find credible Mr. Allison's testimony that a person of ordinary skill in the art "would have had a reasonable expectation of success in combining Denison's electronic key system with Rothbaum's security system" (*see* -345 Ex. 1010 ¶¶ 80–84) because it is consistent with the evidence of record, including Denison's disclosure that security systems using electronic keys were well-known as of the relevant time.[10] *See* -345 Ex. 1002 ¶¶ 3–10; *see also* Ex. 1001, 1:51–58 (the '631 patent disclosing the known use of both "mechanical" and "electrical" keys to arm and disarm "alarm modules or other security devices" in the "Background of the Invention" section). Mr. Allison's testimony and the disclosure of Denison are evidence that implementing electronic keys in security devices was well within the skill level of a person of ordinary skill in the art.

Patent Owner also faults Mr. Allison, Petitioner's declarant, for not having proposed a specific design for the combined system in his declaration. -345 PO Resp. 14–15. However, the Federal Circuit has

> consistently held . . . that "[t]he test for obviousness is not whether the features of a secondary reference may be bodily

[10] Although Mr. Fawcett testifies regarding increased complexity of the proposed Rothbaum-Denison system (Ex. 2010 ¶ 66), we do not find testimony from Mr. Fawcett that rebuts Mr. Allison's testimony regarding reasonable expectation of success.

> incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art."

MCM Portfolio LLC v. Hewlett-Packard Co., 812 F.3d 1284, 1294 (Fed. Cir. 2015) (quoting *In re Keller*, 642 F.2d 413, 425 (CCPA 1981)). Therefore, we discern no requirement for Petitioner to provide evidence of a specific design that allegedly meets the limitations of the claims.

Further, the Supreme Court has held that, "if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill." *KSR*, 550 U.S. at 417. As discussed above, Mr. Allison provides credible testimony that a person of ordinary skill in the art would have had a reasonable expectation of success in combining the teachings of Rothbaum and Denison. *See* -345 Ex. 1010 ¶¶ 80–84. Indeed, as Petitioner points out (-345 Reply 12), Mr. Fawcett testifies that a person of ordinary skill in the art "would have been adept at turning design concepts into working products." -345 Ex. 2010 ¶ 39. Therefore, we are persuaded by Petitioner's contention that a person of ordinary skill in the art would have had a reasonable expectation of success in combining the teachings of Rothbaum and Denison. *See* -345 Pet. 17–19 (citing -345 Ex. 1010 ¶¶ 80–84).

Patent Owner further notes that "[a]ll of the independent claims of the '631 patent require a security device 'attached to an item of merchandise' and an 'alarm' configured to activate in response to the integrity of the security device being compromised." -345 PO Resp. 11. Patent Owner argues that Petitioner "has not truly addressed the underlying fundamental

question of why a [person of ordinary skill in the art] would venture out of the field of merchandise security systems with alarms to vending machines without alarm systems."[11] -345 PO Resp. 12. Patent Owner, therefore, contends Petitioner fails to provide a sufficient rationale to combine Rothbaum and Denison. *See generally id.* at 8–16.

We disagree with Patent Owner. Rather, having considered the arguments of the parties and based on the evidence of record, we are persuaded by Petitioner's contention that a person of ordinary skill in the art would have had reason to combine Denison's teachings of electronic keys and locks with the security system teachings of Rothbaum. *See* -345 Pet. 16–19. In particular, we find that a person of ordinary skill in the art would have been motivated to combine these teachings to take advantage of the numerous benefits of an electronic key system, as described in Denison. *See* -345 Ex. 1010 ¶¶ 76–79; -345 Ex. 1002 ¶¶ 9–10. For example, Denison discloses that "electronic keys provide a greater level of key security compared to mechanical keys, as they cannot be copied as easily as conventional mechanical keys." -345 Ex. 1002 ¶ 9. Denison further discloses that the use of electronic locks and keys "provides advantages in terms of significant reduction in the costs associated with managing the distribution of the keys for unlocking the machines and the monitoring of the usage of the keys" and that "[c]ustomized access limitations may be

[11] Although these arguments may be interpreted as directed to the question of whether Denison is analogous art to the '631 patent, we understand these arguments to be directed instead to the question of whether Petitioner's asserted rationale to combine is sufficient, based on Patent Owner's clarification during oral argument in other cases involving related patents. *See* IPR2016-00899, Paper 29, 95:11–97:2.

programmed by a supervisor into the electronic keys to restrict" their use. *Id.* ¶ 10.

As discussed above, Mr. Allison provides credible testimony explaining that the security device of Rothbaum "is used to protect merchandise in the retail environment" and that, "[i]n this environment, there are also many employees and thus the need for multiple keys, which can get lost or be stolen and then used by unauthorized individuals." -345 Ex. 1010 ¶ 78. Rothbaum itself discloses that "[o]nly authorized personnel should have access to key 40 to prevent the circumvention of the security system" (-345 Ex. 1003, 6:20–22), underscoring the very security issues identified by Mr. Allison that are encountered in a retail environment. *See* -345 Ex. 1010 ¶ 78.

Further, consistent with the evidence of record, including Mr. Allison's testimony, which we credit as discussed above, we find that a person of ordinary skill in the art would have had a reasonable expectation of success in combining Denison's electronic key teachings with the security system of Rothbaum. *See* -345 Ex. 1010 ¶¶ 80–84. We also find that implementing electronic keys in security devices was well within the skill level of a person of ordinary skill in the art. *See id.*

d. Determination of unpatentability of claims 1 and 22

In summary, we find that the combination of Rothbaum and Denison teaches all of the limitations of claims 1 and 22, and we find that a person of ordinary skill in the art would have had reason to, and would have been motivated to, combine the teachings of Rothbaum and Denison in the manner asserted. Patent Owner does not present any objective evidence of nonobviousness as to any of the challenged claims. Having considered the

full record developed during trial, we conclude that Petitioner has shown, by a preponderance of the evidence, that claims 1 and 22 would have been obvious based on Rothbaum and Denison under 35 U.S.C. § 103(a).

5. Dependent Claims 2–5, 8–21, 23–27, and 29

Petitioner further contends the subject matter of dependent claims 2–5, 8–21, 23–27, and 29 would have been obvious based on the combination of Rothbaum and Denison. Pet. 35–51. Although Patent Owner provides specific arguments only with respect to dependent claims 12 and 18 and does not provide specific arguments with respect to claims 2–5, 8–11, 13–17, 19–21, 23–27, and 29 other than those presented for the independent claims in this asserted ground of unpatentability, the burden remains on Petitioner to demonstrate unpatentability of all challenged claims. 35 U.S.C. § 316(e); *see also Dynamic Drinkware LLC, v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015). We have analyzed Petitioner's contentions and supporting evidence in light of the limitations recited in dependent claims 2–5, 8–21, 23–27, and 29, and, as explained more fully below with respect to the particular subject matter recited in the dependent claims, we are persuaded Petitioner has demonstrated unpatentability of these claims over the combined teachings of Rothbaum and Denison. *See* Pet. 35–51.

a. Dependent claims 2–5

Dependent claim 2 recites: "The programmable security system of claim 1, further comprising an attachment cable attached to the security device." Each of dependent claims 3–5 depends from claim 2 and recites further features with respect to the attachment cable of claim 2.

With respect to claim 2, we find the combination of Rothbaum and Denison teaches a programmable security system, as discussed above with respect to claim 1, "further comprising an attachment cable attached to the security device," as asserted by Petitioner. *See* -345 Pet. 35–36 (citing -345 Ex. 1003, 5:54–57, 6:1–4, Fig. 1). In particular, Rothbaum discloses: "Hard goods sensor 24, including a sensor housing 23, is attached to the article 22 . . . . Item cord 28 is of sufficient length to connect the sensor 24 to the alarm circuitry in strip 12." -345 Ex. 1003, 5:62–6:2.

We also find the combination of Rothbaum and Denison teaches that "the alarm is configured to be activated" both "in response to cutting the attachment cable," as recited in claim 3, and "in response to detaching the attachment cable from the security device," as recited in claim 4. *See* -345 Pet. 36–37 (citing -345 Ex. 1003, 10:31–36). In particular, Rothbaum discloses:

> When an alarm condition occurs, i.e., either by removing sensor plug 34 from jack 36, by cutting sensor cable 28, or by removing the sensor 24 from article 22, the alarm horn 126 will sound and the red LED 110 on the strip, which corresponds to the sensor which has been breached, will light.

-345 Ex. 1003, 10:31–36.

We also find the combination of Rothbaum and Denison teaches that "the attachment cable extends between the security device and the item of merchandise," as recited in claim 5. *See* -345 Pet. 37 (citing -345 Ex. 1003, 5:62–63, 6:1–4, Fig. 1). Referring to Figure 1, Rothbaum discloses: "Item cord 28 is of sufficient length to connect the sensor 24 to the alarm circuitry in strip 12. In the preferred embodiment, item cord 28 is coiled to allow for a longer length while minimizing entanglement." Ex. 1005, 6:1–4.

b. Dependent claim 8

Claim 8 depends from claim 1 and recites that "the security device further comprises a visual indicator configured to indicate a status of the security device." Rothbaum discloses:

> A bi-color LED is associated with each sensor circuit and is located on the housing next to the item cord connector. In its secure or non-alarm state, the LED displays a first color, e.g. green, indicating that the system is armed and the item of merchandise is protected. Upon the unauthorized removal of the sensor, the cutting of the item cable, or upon a similar security breach, the alarm will sound and the LED will change from its first color to a second or alarm color (green to red).

-345 Ex. 1003, 3:38–47. Based on this disclosure of Rothbaum, we are persuaded by Petitioner's contentions, and we find, that the combination of Rothbaum and Denison teaches the limitations of claim 8. *See* -345 Pet. 37–38 (citing -345 Ex. 1003, 3:38–47, 13:15–24).

c. Dependent claim 9

Claim 9 depends from claim 1 and recites that "the programmable key comprises a visual indicator configured to indicate a status thereof." Denison discloses that "electronic key 26 also has a light-emitting diode (LED) 38 exposed through a hole in the housing of the key for indicati[ng] the operation status of the key." -345 Ex. 1002 ¶ 37. Based on this disclosure from Denison, we are persuaded by Petitioner's contentions, and we find, that the combination of Rothbaum and Denison teaches the limitations of claim 9. *See* -345 Pet. 38 (citing Ex. 1003 ¶ 37).

d. Dependent claims 10, 16, 17, 19, 21, 23–25, and 29

These claims recite various limitations regarding the logic control circuit's generation and storage of the unique security code.

Claim 17 depends from claim 1 and recites that "the logic control circuit is configured to randomly generate the unique security code." Claim 23, which depends from independent claim 22, recites that "the providing comprises generating the unique security code with the logic control circuit," and claim 24 depends from claim 23 and recites that "the generating comprises randomly generating the unique security code with the logic control circuit."

Petitioner argues Denison teaches that the external computing device randomly generates an access code. -345 Pet. 44, 47–48 (citing -345 Ex. 1002 ¶ 84; -345 Ex. 1010, 56, 67–68). We agree. Denison discloses: "[T]he external computing device 426 may also have programs that implement[] mathematical algorithms for computing the access codes and control parameters. Such calculations may generate the access codes randomly or based on a function that includes the time as a variable." -345 Ex. 1002 ¶ 84. Denison also discloses that the access code is 6 digits having one million possible values. *Id.* ¶ 43 ("The next 6 digits in the key code are the access code (000,000 to 999,999)."). Therefore, we find the combination of Rothbaum and Denison teaches the limitations of claims 17, 23, and 24.

Claim 19 depends from claim 1 and recites that "the unique security code is not chosen by a person." As discussed above, Denison discloses that external computing device 426 randomly generates access codes (-345 Ex. 1002 ¶ 84), and, therefore, any access code so generated is not chosen by a person. Therefore, we find the combination of Rothbaum and Denison teaches the limitations of claims 19. *See* -345 Pet. 46.

Claim 10 recites: "The programmable security system of claim 1, further comprising a switch configured to actuate the logic control circuit for

generating the unique security code." As discussed above, Denison discloses that external computing device 426 (laptop) randomly generates access codes. -345 Ex. 1002 ¶¶ 78, 84. Citing the testimony of its declarant, Mr. Allison, Petitioner contends a person of ordinary skill in the art "would have readily understood from Denison that a keyboard or mouse, both of which contain numerous switches corresponding to the keys/buttons, would be used to cause the generation of the security code and that such use would have been obvious." -345 Pet. 38 (citing -345 Ex. 1010, 49–50). We are persuaded by Petitioner's argument, as supported by the testimony of Mr. Allison and the disclosure of Denison. *See* -345 Ex. 1010, 49–50; -345 Ex. 1002 ¶ 84. Therefore, we find the combination of Rothbaum and Denison teaches the limitations of claim 10.

Claim 16 depends from claim 1 and recites that "the logic control circuit is configured to change the unique security code," and claim 25 recites: "The method of claim 22, further comprising changing the unique security code with the logic control circuit to a new unique security code." Petitioner contends Denison discloses that the key code (having the access code) can be changed and argues that a person of ordinary skill in the art would have understood that this would occur by using the external computing device to generate a new access code. -345 Pet. 43–44, 48–49 (citing -345 Ex. 1002 ¶¶ 51, 84; -345 Ex. 1010, 55–56, 68–69). Denison discloses: "The service person then uses the key learning process described above to change the key code in the memory of the lock to a new value." -345 Ex. 1002 ¶ 51. Therefore, we are persuaded that a key code, which contains the access code (-345 Ex. 1002 ¶ 43), can be changed. Denison further discloses that, following generation of an access code, "external

computing device 426 then wirelessly transmits the *new access code* and/or control parameters to the electronic lock circuit 406." -345 Ex. 1002 ¶ 84 (emphasis added). Denison, therefore, discloses that a key code in a lock can be changed, and it discloses generating and transmitting a new key code to a lock. Based on this disclosure and the testimony of Mr. Allison, we find the combination of Rothbaum and Denison teaches the limitations of claims 16 and 22. *See* -345 Ex. 1010, 55–56, 68–69.

Claim 21 depends from claim 1 and recites that "the logic control circuit comprises a memory for storing the unique security code," and claim 29 recites: "The method of claim 22, further comprising storing the unique security code at the logic control circuit." Petitioner contends Denison discloses that the external computing device stores the access codes in memory. -345 Pet. 46–47, 50–51 (citing -345 Ex. 1002 ¶¶ 79, 84; -345 Ex. 1010, 58–59, 71). We agree. Denison discloses "external computing device 426 has in its memory a timebase, access code or codes for electronic locks on vending machines." -345 Ex. 1002 ¶ 79; *see also id.* ¶ 84 ("To that end, the external computing device may have a database 436 that contains appropriate access codes and control parameters that have been calculated previously for electronic locks, electronic keys, or both."). Therefore, we find the combination of Rothbaum and Denison teaches the limitations of claims 21 and 29.

e. Dependent claim 11

Claim 11 recites: "The programmable security system of claim 1, further comprising a programming station housing the logic control circuit." Petitioner contends that Denison's external computing device teaches "a programming station housing the logic control circuit." -345 Pet. 39 (citing

-345 Ex. 1010, 50–51). We agree. Denison discloses that external computing device 426 is a laptop computer (-345 Ex. 1002 ¶ 78), and we find this disclosure teaches a programming station that houses the logic control circuit, for the reasons discussed above with respect to claim 1.

f. Dependent claim 12

Claim 12 depends from claim 1 and recites that "the security device comprises a port for receiving the programmable key therein." Petitioner points out that Denison's external computing device includes cradle 430 for receiving the electronic key so that the security code can be programmed into the electronic key. -345 Pet. 40–41 (citing -345 Ex. 1002 ¶ 85). With respect to the claimed "security device," Petitioner, with supporting testimony from Mr. Allison, argues:

> A [person of ordinary skill in the art] would have found it obvious to incorporate an infrared port within the modified Rothbaum system disclosed above. Such an infrared port would ensure line of sight between the programmable key and the security device, thereby helping to prevent eavesdropping of the security codes and to prevent accidental disarming of the modified Rothbaum security device.
>
> . . .
>
> A [person of ordinary skill in the art] would have found it obvious to use the same type of key interface in the security device for receiving the programmable key ("electronic key") as used by the programming station ("external computing device"). In other words, it would be obvious to use a "cradle" (*i.e.*, port) for both the programming station and the security device. A [person of ordinary skill in the art] would have been motivated to use the "cradle" for both the programming station and security device, as such would simplify the system and allow for interoperable parts, making repairs and upkeep simpler and more cost efficient.

-345 Pet. 39–40 (citing -345 Ex. 1010, 51–53).

Patent Owner contends that the assertions of Petitioner and Mr. Allison are conclusory and do not show sufficiently why a person of ordinary skill in the art would have modified the combined Rothbaum-Denison system to add a port to the security device for receiving a programmable key. -345 PO Resp. 19–22. Patent Owner further argues that Denison was "greatly concerned about tampering with conventional lock cores" and consequently "shield[ed] the transceiver and lock behind the buttons and door of the vending machine." -345 PO Resp. 22–23 (citing -345 Ex. 1002 ¶¶ 5, 37, 38; -345 Ex. 2007, 3; -345 Ex. 2008, 3, 8). According to Patent Owner, a person of ordinary skill in the art would have been "discouraged from increasing access to the transceiver and lock of Denison by adding a port 'for receiving the programmable key therein.'" -345 PO Resp. 23 (citing -345 Ex. 2010 ¶¶ 80–82). According to Mr. Fawcett, a person of ordinary skill in the art would have been "greatly deterred from adding a port" to the security device to receive a key because "the port would be visually detectable and invite tampering, rather than being hidden behind the buttons." -345 Ex. 2010 ¶ 82.

We disagree with Patent Owner. Petitioner provides sufficient reasoning as to why it would have been obvious to use a cradle (i.e., port) facilitating infrared communication with the electronic key for both the programming station and the security device. *See* -345 Pet. 39 (explaining that doing so would have "help[ed] to prevent eavesdropping of the security codes and to prevent accidental disarming of the modified Rothbaum security device"); -345 Ex. 1010, 51–52. Petitioner's arguments are supported by the disclosure of Denison itself, which teaches infrared

communication between the electronic key and lock and that infrared communication is "preferred because it is directional and short range." -345 Ex. 1002 ¶¶ 9, 37, 77; *see* -345 Pet. 40. Further, Patent Owner's arguments do not address Petitioner's actual proposed combination, which involves modifying Rothbaum's system to use an electronic lock and key rather than a mechanical lock and key. *See* -345 Pet. 39 (explaining proposed modification of Rothbaum's "strip or housing 12" to include port). Unlike the vending machine described in Denison, in Rothbaum's system, "the merchandise is accessible from the outside." *See* -345 Reply 17–18. Thus, we do not agree that a person of ordinary skill in the art would have been deterred from adding a port to the lock that already was attached to the merchandise and accessible.

We conclude that Petitioner has shown, by a preponderance of the evidence, that claim 12 would have been obvious based on Rothbaum and Denison under 35 U.S.C. § 103(a).

g. Dependent claim 13

We are persuaded by Petitioner's argument, and we find, that the combination of Rothbaum and Denison teaches that "the programmable key is configured to wirelessly communicate with the security device," as recited in claim 13. *See* -345 Pet. 41–42 (citing -345 Ex. 1002 ¶ 37 ("The key 26 and the lock preferably communicate with each other wirelessly, which may be via an infrared or radio frequency (RF) channel. In a preferred embodiment, the wireless communications between the key and the lock is via infrared transmissions.")).

h. Dependent claim 14

Claim 14 depends from claim 1 and recites that "the programmable key is configured to be inactivated after a predetermined period of time or a predetermined number of activations." Petitioner contends: "Denison discloses 'operation limits' that can be set for the 'electronic key' (i.e., programmable key) such that the key becomes disabled (inactivated) after a 'number of days' (i.e., predetermined period of time) or 'number of accesses' (i.e., predetermined number of activations)." -345 Pet. 42 (citing -345 Ex. 1002 ¶ 60, Fig. 9).

Denison discloses:

> [A]n electronic key may also be programmed with other types of limits of operation of the key. For instance, the key may be programmed with limit registers that contain values chosen by a supervisor to limit the operation of that particular key. In a preferred embodiment, the limit registers 200 (FIG. 4) are part of the non-volatile memory 52. The operation limits include, for example, time of data, date, *number of days*, number of accesses, number of accesses per day, etc. When the user of the key presses the button on the key to initiate a key code transmission, the microcomputer of the key first compares the limits set in the registers with a real-time clock in the key and an access counter in the key memory. *If any of the limits is exceeded, the key will not transmit the key code to the electronic lock and will terminate the operation.*

-345 Ex. 1002 ¶ 60 (emphases added); *see also id.* at Fig. 9 (illustrating "Key Access Control Limits"). Thus, Denison teaches deactivating the key after any operating limit is exceeded, including "number of days," which teaches a "predetermined period of time." Therefore, we find the combination of Rothbaum and Denison teaches the limitations of claim 14.

i. Dependent claim 15

Claim 15 recites: "The programmable security system of claim 1, wherein the security device further comprises a switch configured to be actuated for activating the alarm in response to the integrity of the security device being compromised." Petitioner argues that Rothbaum's tamper switch 225 causes the horn to activate when the battery compartment is opened and that the integrity of the security device is compromised when the battery compartment is opened. -345 Pet. 43 (citing -345 Ex. 1003, 12:10–18; -345 Ex. 1010, 54–55). We are persuaded by Petitioner's argument, and we find Rothbaum teaches a security device having "a switch configured to be actuated for activating the alarm in response to the integrity of the security device being compromised" based on the following disclosure of Rothbaum:

> As can be seen in FIG. 12, tamper switch 225 is normally open. The tamper switch is activated by the battery compartment screw 224 as can be seen in FIG. 1. If an unauthorized person attempts to tamper with the battery 226, by opening the battery compartment cover 220, they must loosen screw 224. As screw 224 is removed, tension on the activator of switch 225 is moved thus closing switch 225. When switch 225 closes, transistor 122 is turned on thus activating horn 126.

-345 Ex. 1003, 12:10–18. We find that the integrity of the security device is compromised when the battery compartment is opened. *See* -345 Ex. 1010, 54–55. Therefore, we find the combination of Rothbaum and Denison teaches the limitations of claim 15.

j. Dependent claim 18

Claim 18 recites: "The programmable security system of claim 1, wherein the unique security code is unique to a particular retail

establishment or retail store." Petitioner contends that a person of ordinary skill in the art would have understood and found obvious that a retail establishment employing the Rothbaum system, as modified by the teachings of Denison, would not share the system, including the external computing device that generates the access code, with other retail stores. -345 Pet. 45 (citing -345 Ex. 1010, 56–57). Petitioner further argues that, because the access code of Denison's external computing device 426 is generated randomly and is one of one million possible numbers, it is "unique" to the particular retail store. *Id.* For generation of the "unique" security code, as set forth in parent claim 1, Petitioner relies in part on Denison's teaching that the key code stored in an electronic key includes seven digits, with six of the digits being the access code. -345 Pet. 21, 45; -345 Ex. 1002 ¶ 43 ("The next 6 digits in the key code are the access code (000,000 to 999,999).").

Patent Owner argues Petitioner has "failed to show how the additional limitation of being 'unique to a particular retail establishment' or store are met by Denison's randomly generated code." -345 PO Resp. 25. According to Patent Owner, Petitioner and its declarant, Mr. Allison, "point to nothing in Rothbaum or Denison that supports or suggests limiting the system or randomly generated code to a particular retail store or establishment." *Id.* at 26.

We disagree. Rather, we find Petitioner's reasoning and cited evidence to be persuasive. In particular, we are persuaded that a person of ordinary skill in the art would have understood, or at minimum found obvious, that a retail establishment would not share the system, including the device that performs the programming, with other retail stores. *See* -345 Ex.

1010, 56. Not sharing the system or its components with other stores is consistent with Rothbaum's disclosure that "[o]nly authorized personnel should have access to key 40 to prevent the circumvention of the security system." -345 Ex. 1003, 6:20–22. The random generation of an access code, with one million different possible outcomes (ranging from zero to 999,999, inclusive), as taught by Denison, supports Petitioner's position that the security (access) code is unique to the logic control circuit and, therefore, unique to the particular retail establishment or retail store employing that particular logic control circuit.

Petitioner, therefore, has demonstrated by a preponderance of the evidence that claim 18 would have been obvious based on the combination of Rothbaum and Denison.

k. Dependent claim 20

Claim 20 recites: "The programmable security system of claim 1, wherein the programmable key is configured to provide the unique security code to the security device for storing the unique security code." Petitioner relies on Denison's description of a "learning mode, in which the electronic lock receives a key code transmitted from an electronic key." -345 Pet. 46 (quoting -345 Ex. 1002 ¶¶ 7, 45). We are persuaded that this "learning mode" of Denison teaches that the "key is configured to provide the unique security code to the security device for storing the unique security code." *See also* -345 Ex. 1002 ¶ 6 ("[T]he present invention provides a vending machine with a field-programmable electronic lock. The electronic lock can *learn a key code from a corresponding electronic key*, a hand-held program unit, and/or an external computing device via wireless communications."

(emphasis added)). Therefore, we find the combination of Rothbaum and Denison teaches the limitations of claim 20.

l. Dependent claim 26

Claim 26 recites: "The method of claim 22, wherein the controlling comprises disarming the security device upon a matching of the unique security code provided by the logic control circuit with the unique security code stored by the security device." Petitioner cites, in part, the following disclosure of Denison:

> The key codes in the keys and the locks of the vending machines are used to define the security and access control strategy of the electronic lock system. Each electronic key 26 has a key code 88 stored therein, and the same key code is stored in the memory 52 of the electronic lock in each vending machine to be operated with the electronic key. During each access attempt, the key code in the electronic key is transferred from the key to the electronic lock using a secured communication method. The electronic lock can be unlocked if the key code it receives from the electronic key matches the key code stored in the memory of the lock.

-345 Ex. 1002 ¶ 42, *quoted in* -345 Pet. 49. Petitioner contends, therefore, that, in the modified Rothbaum-Denison system, "disarming occurs upon a matching of security codes stored by the security device and with the code that was provided by the logic control circuit (and then stored by the programmable key)." -345 Pet. 50 (citing -345 Ex. 1010, 70). We find Denison discloses unlocking upon a matching of security codes, as described above, and we find the combination of Rothbaum and Denison teaches the limitations of claim 26.

m. Dependent claim 27

We are persuaded by Petitioner's argument, and we find, that the combination of Rothbaum and Denison teaches "communicating the unique security code to the programmable key," as recited in claim 27. *See* -345 Pet. 50 (citing -345 Ex. 1002 ¶ 85 ("To that end, the electronic key 410 is connected to the cradle 430, and the access code that has been programmed into the lock is transmitted via the cradle into the key . . . .")).

n. Determination of unpatentability of dependent claims 2–5, 8–21, 23–27, and 29

In summary, we find the combination of Rothbaum and Denison teaches the limitations of dependent claims 2–5, 8–21, 23–27, and 29, and, for the reasons discussed with respect to independent claims 1 and 22, we find a person of ordinary skill in the art would have had reason to, and would have been motivated to, combine the teachings of Rothbaum and Denison. Having considered the full record developed during trial, we conclude that the subject matter of dependent claims 2–5, 8–21, 23–27, and 29 would have been obvious based on the combined teachings of Rothbaum and Denison.

E. Unpatentability Challenge Based on Rothbaum, Denison, and Ott (§ 103(a) – Claims 6 and 7)

Claim 6 depends from claim 2 and recites that the security system comprises "a recoiler connected to the attachment cable," and claim 7 recites that "the recoiler is located within the security device." Petitioner asserts claims 6 and 7 would have been obvious based on the combination of Rothbaum, Denison, and Ott. -345 Pet. 7, 51–55.

Ott is directed to an apparatus for "safeguarding a merchandise item against theft, having a safeguarding part for fixing to the merchandise item and having a connecting cord for connecting the safeguarding part to an object which is not at risk of theft." -345 Ex. 1004, 1:5–9. Figure 9 of Ott is reproduced below.

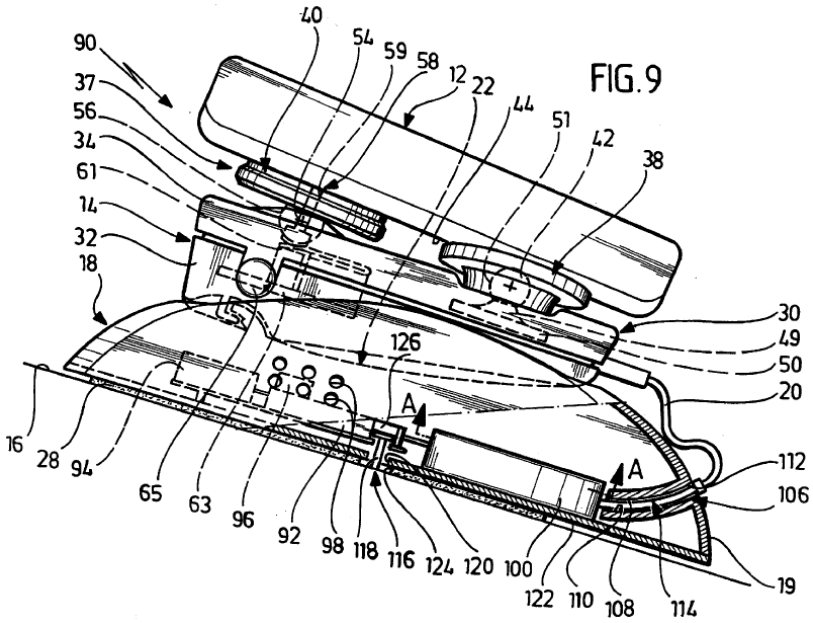


Figure 9 of Ott depicts apparatus 90 having holding part 18 affixed to an object such as lid 16 of a display case and having safeguarding part 14, which can be attached to item of merchandise 12. -345 Ex. 1004, 7:26–40, 11:43–12:2. Ott further discloses:

> The monitoring circuit 92 is electrically connected to the switching element 61 via the connecting cord 20. In order to automatically wind up the connecting cord 20, *a winding element 100 is disposed within the housing 19 of the holding part 18 and winds up the connecting cord 20 as far as possible*. To that end, the winding element 100—as becomes clear from FIG. 10, in particular—comprises a coil 102, which is mounted in a rotatable manner and accommodates a spiral spring 104 and onto which the connecting cord 20 can be wound up. The connecting cord 20 can be unwound counter to the effect of the

> spiral spring 104 if a customer, for example for the purpose of subjecting the merchandise item 12 to be monitored to a test use, removes the merchandise item 12 with the safeguarding part 14 fitted thereto from the holding part 18. If the customer then puts the merchandise item 12 back again, the winding element 100 ensures that the connecting cord 20 is wound up on account of the spring force of the spiral spring 104 on the coil 102.

-345 Ex. 1004, 11:16–33 (emphasis added).

Petitioner contends Ott's "winding element 100" teaches a "recoiler" as claimed, and Petitioner argues a person of ordinary skill in the art would have been motivated to use a winding unit in the modified Rothbaum-Denison system. -345 Pet. 52–53. In particular, Petitioner contends:

> [A person of ordinary skill in the art] would have been motivated to include Ott's "winding unit 100" (i.e., recoiler) within the "strip or housing 12" of the modified Rothbaum system or alternatively to modify (or replace) the "strip or housing 12" in the modified Rothbaum system with a security device as disclosed in Ott, including the "winding unit 100." A [person of ordinary skill in the art] would have been motivated to use Ott's "winding unit 100" in the modified Rothbaum system because it allows an item of merchandise to be picked up an[d] examined by a customer, yet still secured by an attachment cable. The item of merchandise can then be set with the attachment cable retracting. A [person of ordinary skill in the art] would have found this highly advantageous since it provides for sufficient security, yet still maintains a neat and professional appearance, since a long attachment cable is not drooping over a display table and only the required portion is displayed at any given point.

-345 Pet. 52–53 (citing -345 Ex. 1010 ¶¶ 118–121).

Patent Owner argues Petitioner fails to show why a person of ordinary skill in the art would have used Ott's recoiler in the Rothbaum-Denison

combination. -345 PO Resp. 27–28. Patent Owner argues Petitioner's asserted rationale to combine relies only on Mr. Allison's testimony and further argues that "Mr. Allison makes no efforts to examine the details of *any* of the prior art and instead makes up a justification that he subjectively believes would provide the necessary motivation." -345 PO Resp. 27. We disagree. Mr. Allison testifies:

> [A person of ordinary skill in the art] would have been motivated to use Ott's "winding unit 100" in the modified Rothbaum system because it allows an item of merchandise to be picked up and examined by a customer. At the same time, the merchandise is still secured by an attachment cable for security purposes. The item of merchandise can then be set down (e.g., on the stand of Ott as shown in Figure 9 above, on a display table, etc.) with the attachment cable retracting.
>
> A person of ordinary skill in the art] would have found a system, as discussed in the previous paragraph, highly advantageous since it provides for sufficient security, but also maintains a professional and neat appearance. Without a recoiler or retractor to allow the customer to pick up the merchandise would otherwise require a long attachment cable, which would easily become disorganized, for example, drooping over the display table and perhaps obstructing the merchandise. In using a retractor with a recoiler, only the required portion is extended at any given point.

-345 Ex. 1010 ¶¶ 119–120. Ott discloses that the connecting cord is unwound when a customer picks up the item and that, "[i]f the customer then puts the merchandise item 12 back again, the winding element 100 ensures that the connecting cord 20 is wound up on account of the spring force of the spiral spring 104 on the coil 102." -345 Ex. 1004, 11:25–33. Ott's disclosure that the recoiler winds the connecting cord back up supports Mr. Allison's testimony that inclusion of a recoiler provides a "professional and neat appearance" and keeps a long attachment cable from becoming

disorganized. *See* -345 Ex. 1010 ¶¶ 119–120. Therefore, we do not agree that Mr. Allison's testimony is conclusory. Rather, we find Mr. Allison's testimony is supported by the disclosure of Ott itself.

Patent Owner also argues Petitioner "does not bother to address the advantages provided by the 'strip or housing' in the modified Rothbaum system and whether modification or replacement of the strip or housing is something that a person of ordinary skill in the art would entertain." -345 PO Resp. 28. We disagree because Petitioner expressly argues that a person of ordinary skill in the art would have been motivated to modify the system to include a recoiler for the reasons discussed above. *See* -345 Pet. 52–53; -345 Ex. 1010 ¶¶ 118–120.

Patent Owner further argues Petitioner "never describes how Ott's winding unit would be used to modify Rothbaum's strip or housing" or "what the Rothbaum/Denison combination would look like if the Rothbaum's strip or housing were replaced by Ott's winding unit 100." -345 PO Resp. 28. As we discuss above with respect to claim 1, however, we discern no requirement for Petitioner to provide evidence of a specific design that allegedly meets the limitations of the claims. *See MCM*, 812 F.3d at 1294.

With respect to claim 7, Patent Owner argues that, even if adding a recoiler to the Rothbaum-Denison system were obvious, "the most likely solution would be to plug the recoiler directly into the strip [or] housing." -345 PO Resp. 29 (citing Ex. 2019 ¶¶ 3–5). In support of its contention, Patent Owner cites another reference, U.S. Patent Application Publication No. 2005/0001485 A1 (Ex. 2017, "Pail"), as allegedly showing recoiler unit 7A outside, rather than within, a base unit. -345 PO Resp. 29 (citing -345

Ex. 2017 ¶¶ 27–31, Fig. 2; -345 Ex. 2019 ¶ 4). According to Patent Owner, "both Ott and Pail teach connecting cables *to* the central unit rather than placing recoilers *within* the central unit." -345 PO Resp. 29 (citing -345 Ex. 2019 ¶ 4).

As an initial matter, we disagree with Patent Owner's characterization of Ott because Ott expressly describes that winding unit 100 ("recoiler") is located within the housing of holding part 18: "In order to automatically wind up the connecting cord 20, a winding element 100 is disposed within the housing 19 of the holding part 18 . . . ." -345 Ex. 1004, 11:17–20, Fig. 9. Thus, we agree with Petitioner that "Ott discloses that the 'winding element' is located within the 'housing 19 of the holding part 18' (*i.e.*, within[] the security device)." -345 Pet. 55 (citing -345 Ex. 1004, 11:16–21).

Furthermore, Pail's disclosure of a different configuration shows that there are multiple known options for placement of a recoiler in a security system available to a person of ordinary skill in the art. *See KSR*, 550 U.S. at 421 ("When there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp."). Furthermore, even if a different solution would have been more likely based on the prior art, as Patent Owner suggests (-345 PO Resp. 29), the Federal Circuit has stated that the "case law does not require that a particular combination must be the preferred, or the most desirable, combination described in the prior art in order to provide motivation for the current invention." *In re Fulton*, 391 F.3d 1195, 1200 (Fed. Cir. 2004).

Patent Owner's declarant, Mr. Fawcett, also cites Pail and testifies that the "the most likely solution" would be to keep the recoiler external to

the security device. -345 Ex. 2019 ¶¶ 3–6. In particular, Mr. Fawcett testifies:

> A person of ordinary skill would not, reading the Ott patent, decide to put the recoiler within the strip housing of Rothbaum. A person of ordinary skill would have done exactly as Ott suggests and leave the recoiler external to the strip housing. The person of ordinary skill in the art would connect the recoiler to the strip housing via a cable, coming from the recoiler, that plugs into one of the jacks on the strip housing.

-345 Ex. 2019 ¶ 5. As discussed above, however, Ott describes that the recoiler is located within the housing of holding part 18, and, therefore, Petitioner's proposed modification of including a recoiler within the housing of the security device simply would be doing what Ott expressly describes. -345 Ex. 1004, 11:17–20, Fig. 9.

Patent Owner further argues that locating recoilers within the housing of the Rothbaum security device "would eliminate Rothbaum's three position slide switch," which, according to Patent Owner, the applicants for the Rothbaum patent described as having certain advantages. -345 PO Resp. 30–31 (citing -345 Ex. 1003, 7:58–62, claim 1, Figs. 14–15; -345 Ex. 2018, 15–16). Simply because there are disadvantages to a proposed modification, however, does not mean that there would be no reason for the modification. *Medichem*, 437 F.3d at 1165 ("[A] given course of action often has simultaneous advantages and disadvantages, and this does not necessarily obviate motivation to combine."). In response to Patent Owner's arguments and Mr. Fawcett's testimony, Mr. Allison testifies that whether it is preferable to locate a recoiler inside or outside of a security device's housing depends on the circumstances. -345 Ex. 1015 ¶ 18. For example, according to Mr. Allison, if the housing of the security device "is in sight of customers,

it would be undesirable for the recoiler to be visible to those customers" because it "would completely eliminate the recoiler's benefit of providing a professional and neat appearance." *Id.* Furthermore, Mr. Allison testifies that a person of ordinary skill in the art "would have understood that having a 'jack 36' or 'slide switch' is not a necessary requirement in creating a security device that alarms." *Id.* ¶ 19.

Based on the evidence of record, including Mr. Allison's testimony and Ott's express disclosure of including a recoiler inside of the housing of a security device (-345 Ex. 1004, 11:17–20, Fig. 9), we conclude that locating a recoiler within the security device would have been obvious to a person of ordinary skill in the art. *See* -345 Ex. 1010 ¶¶ 118–120; -345 Ex. 1015 ¶ 18.

Based on the foregoing and having considered the full record developed during trial, we conclude that the subject matter of dependent claims 6 and 7 would have been obvious based on the combined teachings of Rothbaum, Denison, and Ott.

F. Unpatentability Challenge Based on Rothbaum, Denison, and Roatis (§ 103(a) – Claim 28)

Claim 28 recites: "The method of claim 27, wherein the communicating comprises wirelessly communicating the unique security code to the programmable key." Petitioner asserts claim 28 would have been obvious based on the combination of Rothbaum, Denison, and Roatis. -345 Pet. 7, 56–60.

Petitioner first contends that Denison teaches that the external computing device transmits the access code to the electronic key via cradle 30 using wireless communication. -345 Pet. 56 (citing -345 Ex. 1002 ¶¶ 41, 78, Fig. 4; -345 Ex. 1010 ¶¶ 125–128). In support, Petitioner and Mr.

Allison rely on Denison's disclosure that "electronic key 26 includes . . . a half-duplex [Infrared Data Association (IRDA)] infrared communication interface 84 for communicating with the electronic lock of a vending machine or with a computer for programming the key." -345 Ex. 1002 ¶ 41. According to Mr. Allison, "Denison describes no communication interface in the electronic key other than infrared. Thus, it is apparent that any communication between the 'cradle' and 'electronic key' must be wirelessly through the 'IRDA communication interface 84.'" -345 Ex. 1010 ¶ 128 (citing -345 Ex. 1002, Fig. 4).

We are persuaded, and we find, that Denison teaches "wirelessly communicating the unique security code to the programmable key," as recited in claim 28, because Denison describes that the infrared communication interface of the key is "for communicating with . . . a computer for programming the key." -345 Ex. 1002 ¶ 41. Thus, Denison describes using wireless communication (infrared) to program the key, and, as discussed above with respect to claim 27, Denison discloses that programming the key involves transmitting the access code ("unique security code") to the key. -345 Ex. 1002 ¶ 85 ("To that end, the electronic key 410 is connected to the cradle 430, and the access code that has been programmed into the lock is transmitted via the cradle into the key . . . ."). We agree with Petitioner and Mr. Allison that the only mechanism by which the electronic key in Denison communicates is wireless; there is no non-wireless communication disclosed. *See* -345 Pet. 56; -345 Ex. 1010 ¶¶ 127–128.

Petitioner further argues Roatis discloses a cradle that communicates wirelessly with an electronic key. -345 Pet. 56–57 (citing -345 Ex. 1005

¶¶ 69, 80, 129). Petitioner contends that, "[r]egardless of whether Denison discloses a wireless cradle, a [person of ordinary skill in the art] would have found it obvious to modify Denison to use Roatis's wireless cradle." -345 Pet. 57.

Roatis discloses a system for "managing electronic keys used for accessing vending machines or the like and for managing audit data collected by the electronic keys from the vending machines." -345 Ex. 1005 ¶ 68. Figure 1 of Roatis is reproduced below.

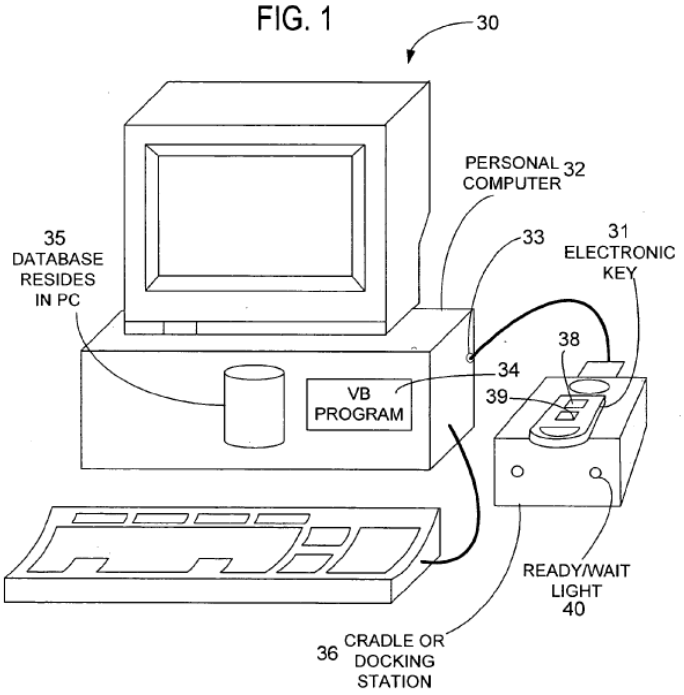


Figure 1 depicts personal computer 32 and cradle 36, which communicates wirelessly with electronic key 31 when push button 39 is pressed. *Id.* ¶¶ 68–69. Cradle 36 has "a receiving place for receiving the electronic key, and indicators such as a ready/wait light 40," which may be red, for example, when the cradle is communicating with the electronic key. *Id.* ¶¶ 69, 80. Personal computer 32 may display a user interface screen for setting parameters and programming the electronic key. *Id.* ¶ 80, Fig. 5B.

We find Roatis is analogous to the claimed invention because, as discussed with respect to Denison, using electronic keys and locks with vending machines is in the same field of endeavor as the '631 patent, namely protecting merchandise from theft, and Roatis is directed to "managing electronic keys used for accessing vending machines." -345 Ex. 1005 ¶ 68. We also are persuaded by Petitioner's arguments that Roatis teaches "wireless" communication with the key. *See* -345 Pet. 56–57; -345 Ex. 1005 ¶¶ 69 (disclosing "wireless transmission" from the key and an "interface device for forwarding and receiving communications to and from [the] electronic key"), 129, claim 2 ("the cradle communicates with the key through wireless transmissions").

Petitioner argues that a person of ordinary skill in the art "would have found advantageous the fact that with Roatis's cradle the electronic key does not need to be physically connected to the cradle, but instead simply needs to be 'within communication distance.'" -345 Pet. 57 (quoting -345 Ex. 1005 ¶ 80; citing -345 Ex. 1010 ¶¶ 132–133). As such, Petitioner argues that a person of ordinary skill in the art "would have been motivated to combine the references by replacing Denison's cradle with Roatis's cradle for its wireless advantages." -345 Pet. 57. We are persuaded that Petitioner has set forth sufficiently articulated reasoning with rational underpinning, supported by evidence in the record, for its combination of Rothbaum, Denison, and Roatis. *See* -345 Ex. 1010 ¶¶ 132–134.

Based on the foregoing and having considered the full record developed during trial, we conclude that the subject matter of dependent claim 28 would have been obvious based on the combined teachings of Rothbaum, Denison, and Roatis.

G. Unpatentability Challenge Based on Uchida
(§ 102(b) – Claims 1–5, 8–11, 13, 15, 16, 18, 19, 21–23, and 25–29)

Petitioner contends Uchida anticipated claims 1–5, 8–11, 13, 15, 16, 18, 19, 21–23, and 25–29 and relies on the testimony of Mr. Allison in support of its contentions. -344 Pet. 9, 36–53; -344 Ex. 1017.

1. Overview of Uchida

Uchida is directed to a merchandise security system, such as that depicted in Figure 8, reproduced below.

【図８】

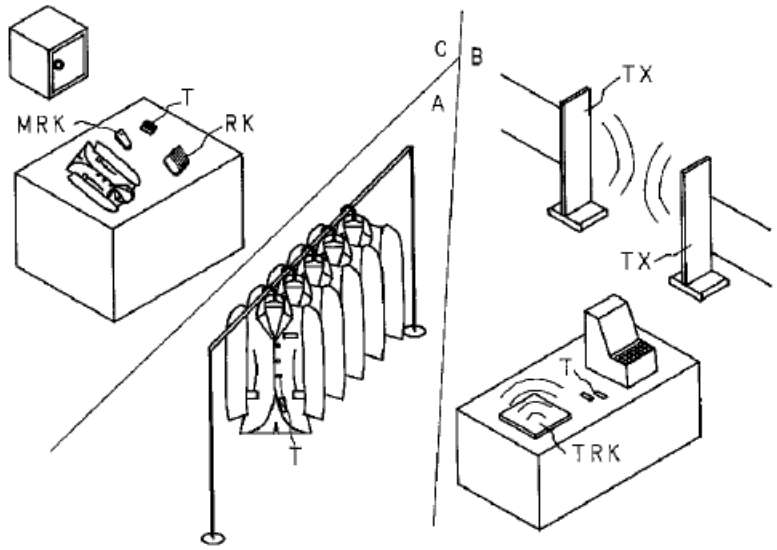


Figure 8 illustrates the main parts of a theft prevention system according to Uchida. -344 Ex. 1004 ¶ 74. Theft prevention tag T is attached to a product to be protected, such as an article of clothing. *Id.* Master instruction signal transmission device (hereinafter, "MRK device"[12]) has a microcomputer that

[12] Uchida describes two types of "master remote control key[s]." Uchida refers to the "master instruction signal transmission device" as a "handy type" master remote control key and designates it "MRK." -344 Ex. 1004 ¶¶ 63, 70. Uchida also describes a device labeled "TRK" as a "desktop type

sets encryption codes used as part of a reset code to disable the alarms in the theft prevention tags. *Id.* ¶¶ 47, 66. The system also employs "handy type" remote control key (RK) for transmitting set and reset codes to individual theft prevention tags. *Id.* ¶¶ 67–68.

2. Independent Claims 1 and 22

Petitioner contends Uchida's system using theft prevention tags discloses a "programmable security system for protecting items of merchandise from theft" and a "method for protecting items of merchandise from theft," as recited in the preambles of independent claims 1 and 22, respectively. -344 Pet. 37–38, 44–45 (citing -344 Ex. 1004 ¶ 1, Fig. 8; -344 Ex. 1017, 52). We are persuaded Uchida's merchandise security system describes this subject matter. *See* -344 Ex. 1004 ¶ 1, Fig. 8.

a. Logic control circuit

With respect to the "logic control circuit" limitations of claims 1 and 22, Petitioner contends "'microcomputer 10' and other components such as 'LC resonance circuit 13'" in the MRK device provide an encryption code, which Petitioner argues discloses a "unique security code" that is "unique to the logic control circuit." -344 Pet. 38–41 (citing -344 Ex. 1004 ¶¶ 20, 63, 66, 67, 123, Figs. 3, 4, 7; -344 Ex. 1017, 52–55). In particular, Uchida discloses:

> When the encryption switch (CRS) has been operated, the microcomputer 10 changes the setting of the encryption

---

master remote control key." *Id.* ¶ 74. For clarity of the record, we refer to the master instruction signal transmission device, which Petitioner alleges describes the claimed "logic control circuit," as the "MRK device." Petitioner does not rely on the device labeled TRK as describing any of the claim limitations.

> code included in the reset code to a new encryption code in accordance with the operation. When the encryption change button (CRB) has been operated, the microcomputer 10 modulates an encryption change code for instructing change to the encryption code that is set through the LC resonance circuit 13 and transmits the code.

-344 Ex. 1004 ¶ 66. In Figure 7, Uchida discloses that the encryption code is four digits of the "reset code." -344 Ex. 1004 ¶ 73, Fig. 7. Uchida further discloses that the system is "capable of setting a different reset code for each store." Ex. 1004 ¶ 20; *see also id.* ¶ 125 ("According to the theft prevention device as in invention 8, a different reset code for the theft prevention tags can be set for each store, and theft can be further securely prevented.").

Patent Owner makes two arguments with respect to this claim limitation, namely that Petitioner has not shown (1) that Uchida's encryption code is "unique to the logic control circuit" or (2) that Uchida discloses that the encryption code is provided by the logic control circuit. -344 PO Resp. 7–9.

Patent Owner's second argument is premised on its assertion that "the claim term *providing* is not directed to communicating among devices in the system." -345 PO Resp. 9 (citing -345 Dec. on Inst. 5–6). We disagree with this assertion because, as discussed above in the section addressing claim construction, although providing is not limited to particular forms of communication, communicating a code is, nonetheless, within the scope of providing the code. *See supra* Section II.A.3. Patent Owner notes that Petitioner "and Mr. Allison have asserted that 'Uchida does not disclose how the "encryption code" is generated.'" -344 PO Resp. 9 (quoting -344 Pet. 59, -344 Ex. 1017, ¶ 125; citing Ex. 2014, 30:12–17). According to Patent Owner, "[t]hese are admissions that Uchida *cannot anticipate* Claims 1

and 22." *Id.* We disagree because Uchida expressly discloses that microcomputer 10 changes the encryption code and transmits the code. -344 Ex. 1004 ¶ 66. Although Uchida does not describe expressly how the code is generated, it still describes providing the code at least by transmitting the code to other devices in the system.

As to its first argument, Patent Owner contends Petitioner has not shown that the encryption code, which is "a four-digit binary number, with 16 different possible variations, is 'unique,' and, in particular, is unique 'to the logic control circuit.'" -344 PO Resp. 8. Patent Owner further asserts: "[Petitioner] does not provide any support as to how Uchida's alleged logic control circuit—the 'master remote control key (MRK)' and its 'LC resonance circuit 13' provides a security code unique to the logic control circuit/MRK. At best, [Petitioner] is arguing obviousness, not anticipation." -344 PO Resp. 8.

As noted above, Uchida describes setting a different reset code for each store. -344 Ex. 1004 ¶¶ 20, 125. Because the reset code (including the encryption code) is different for each store, each store's reset code is "unique" to that store. Of course, if there are more than 16 stores using a system in which the encryption code is one of 16 possible values, then there will be overlap in the codes, and, in that situation, a particular code will not be unique to a particular store among all the stores employing the system. But this is a possibility in any system of finite codes. Here, Uchida unequivocally discloses "setting a different reset code for each store" (-344 Ex. 1004 ¶ 20), and, therefore, we find Uchida discloses that its encryption code is unique to each store. Claims 1 and 22, however, recite a further

qualifier on the uniqueness of the security code, namely that it be "unique to the logic control circuit."

In Uchida, if each store has one MRK device that provides the encryption code, then the encryption code that is unique to the store also would be unique to the MRK device given the one-to-one correspondence of store to MRK device in this scenario. Although Uchida does not state expressly whether each store has one or more MRK devices, anticipation does not require the limitation at issue to be expressly stated, *ipsissimis verbis*, in a prior art reference. Rather, the test may be satisfied if one with ordinary skill in the art would have understood from the prior art reference that what is required by the claim limitation is disclosed. "'[T]he dispositive question regarding anticipation [i]s whether *one skilled in the art* would reasonably understand or infer from the [prior art reference's] teaching' that every claim element was disclosed in that single reference." *Dayco Prods., Inc. v. Total Containment, Inc.*, 329 F.3d 1358, 1368 (Fed. Cir. 2003) (alterations in original) (quoting *In re Baxter Travenol Labs.*, 952 F.2d 388, 390 (Fed. Cir. 1991)); *see also Wasica Fin. GmbH v. Cont'l Auto. Sys., Inc.*, 853 F.3d 1272, 1284 (Fed. Cir. 2017) ("Anticipation is an inquiry viewed from the perspective of one skilled in the art."); *Scripps Clinic & Research Foundation v. Genentech, Inc.*, 927 F.2d 1565, 1576 (Fed. Cir. 1991) ("[Anticipation requires that there be] no difference between the claimed invention and the reference disclosure, as viewed by a person of ordinary skill in the art in the field of the invention."), *overruled in part on other grounds by Abbott Labs. v. Sandoz, Inc.*, 566 F.3d 1282, 1293 (Fed. Cir. 2009).

Uchida discloses that the MRK device is the "master instruction signal transmission device" that changes the encryption code and provides the encryption code to the other devices. -344 Ex. 1004 ¶¶ 63, 66. Uchida discloses that "the desktop type [(master remote control key)] is not provided with an encryption switch (CRS) for setting the encryption code and an encryption change button (CRB) for instructing change of the encryption code" but, rather, "receiv[es] encryption change code signals from the handy type master remote control key (MRK)." -344 Ex. 1004 ¶ 70. Furthermore, the remote control key (RK) does not have an encryption switch (CRS) for changing the encryption code; rather, it "transmits only the set code and reset code to the VS type and WT type theft prevention tag described above using radio waves" and receives an encryption code from the MRK device. -344 Ex. 1004 ¶ 67, Fig. 4. Thus, the system of Uchida relies on the MRK device to provide the encryption code that is unique to the store, and Uchida does not describe a situation in which a store has more than one MRK device. In addition, Uchida describes that the MRK device "is usually securely stored in a safe" and is accessed by "a person in charge" to change the encryption code. -344 Ex. 1004 ¶ 75. Thus, the security of the MRK device is paramount, and having multiple MRK devices in a store that could be used to reprogram the other security devices increases the possibility of security issues and potential for conflicting encryption codes within the store. Therefore, although there is nothing in Uchida that expressly prohibits multiple MRK devices in one store, in view of the full disclosure of Uchida, we find that a person of ordinary skill in the art would have understood Uchida as describing a system to be used in a store in which there is one MRK device that provides an encryption code for the

remaining devices in that store. Because the encryption code is unique to that store, it is also unique to the MRK device of that store.

Based on the foregoing, we find Uchida describes "a logic control circuit configured to provide a unique security code, the unique security code being unique to the logic control circuit," as recited in claim 1, and "providing a unique security code with a logic control circuit, the unique security code being unique to the logic control circuit," as recited in claim 22. -344 Ex. 1004 ¶¶ 66–67, Fig. 3; -344 Ex. 1017, 52–55.

b. Programmable key

Petitioner contends that Uchida's "remote control key (RK)" has a memory that stores the encryption code and, therefore, discloses "a programmable key comprising a memory configured to store the unique security code," as recited in claim 1, and "storing the unique security code at a programmable key," as recited in claim 22. -344 Pet. 41, 45 (citing -344 Ex. 1004 ¶¶ 34, 67, 68; -344 Ex. 1017, 55–56). We are persuaded because, in reference to Figure 4, which depicts the remote control key, Uchida discloses that "[t]he 4-bit microcomputer 10 stores an encryption code that should be included in the reset code, and when the LC resonance circuit 14 receives an encryption change code signal, the code is updated to a new encryption code." -344 Ex. 1004 ¶ 68. Therefore, we find Uchida describes these limitations of claims 1 and 22.

c. Security device

Claim 1 further recites: "a security device comprising an alarm and a memory for storing the unique 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." Independent claim 22 similarly recites: "storing the unique security code at a security device attached to an item of merchandise, the security device comprising an alarm configured to be activated in response to the integrity of the security device being compromised."

Petitioner contends Uchida's theft prevention tag (T) describes the claimed "security device." -344 Pet. 41–43. Petitioner argues Uchida discloses that the theft prevention tag is attached to merchandise such as clothing and that it has a memory that stores the encryption code and has a flashing LED and a buzzer. -344 Pet. 41–43 (citing -344 Ex. 1004 ¶¶ 35, 36, 43, 51, 60, Fig. 2; -344 Ex. 1017, 56–57). Petitioner further contends Uchida discloses that the LED and the buzzer (i.e., the claimed "alarm") in the theft prevention tag are activated when the attachment wire is cut, thereby disclosing that "the security device [is] further configured to activate the alarm in response to the integrity of the security device being compromised," as recited in claim 1. Pet. 41–42 (citing Ex. 1004 ¶¶ 35, 36, 43, 60). We are persuaded by these contentions.

Figure 2 of Uchida is reproduced below.

【図２】fig. 2

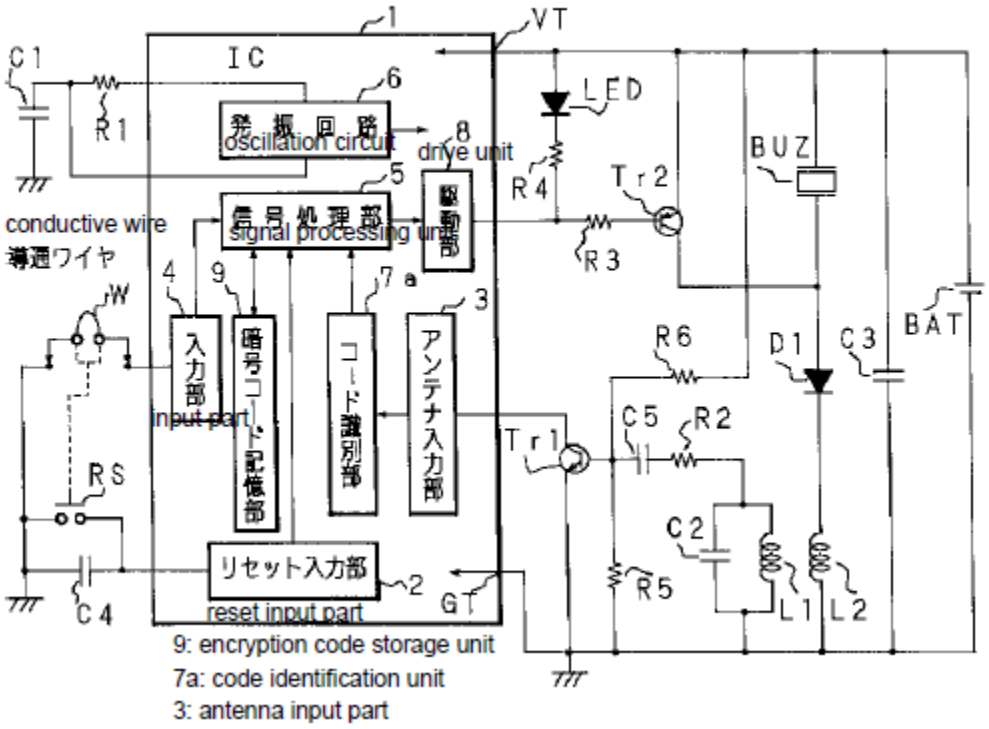


Figure 2 is a block diagram illustrating the components of one type of theft prevention tag referred to in Uchida as a "WT type" or "VT type." -344 Ex. 1004 ¶¶ 43–44, 60. Figure 2 shows a light emitting diode (LED) and a buzzer (BUZ), and it also shows element 9 as an encryption code storage unit. -344 Ex. 1004, Fig. 2; *see id.* ¶ 75 ("The remote control key (RK) and theft prevention tags (T) receive the encryption change code signal, and update[] the encryption code stored in each of the encryption storage means (C)."). Uchida further discloses:

> [W]ith the VT type theft prevention tag, if a person attempts to detach the theft prevention tag from the theft prevention object by cutting the conductive wire W to avoid the matter described above when in the set mode, the signal processing unit 5 recognizes the signal thereof through the input part 4, outputs a warning signal to the drive unit 8, and sets the theft prevention tag to alarm mode. The warning signal causes the light-

> emitting diode (LED) to flash due to the output terminal of the drive unit 8 becoming an L level signal at, for example, 8Hz. At this time, the drive unit 8 superimposes a 4 kHz warning signal to the 8 Hz L level signal, drives the transistor TR2 and causes the buzzer (BUZ) to sound.

-344 Ex. 1004 ¶ 60. In Figure 1, Uchida describes a "VS type theft prevention tag" that also has an encryption code storage unit, a light emitting diode, and a buzzer. -344 Ex. 1004 ¶¶ 35–36, 46, 53, Fig. 1.

Therefore, Uchida discloses a theft prevention tag that (1) stores an encryption code (i.e., the claimed "unique security code"), (2) is attached to a theft prevention object (i.e., the claimed "item of merchandise"), and (3) has an alarm that is activated when the conductive wire is cut (i.e., the claimed "in response to the integrity of the security device being compromised"). As such, we find that Uchida describes the "security device" limitations of claims 1 and 22.

d. Controlling the security device

Claim 1 further recites: "wherein the programmable key is configured to control the security device upon a matching of the unique security code stored in the memory of the security device with the unique security code stored by the programmable key." Independent claim 22 similarly recites: "controlling the security device upon a matching of the unique security code provided by the logic control circuit with the unique security code stored by the security device."

Petitioner contends Uchida discloses that the remote control key (i.e., the claimed "programmable key") sends a reset code containing the encryption code to the theft prevention tag and that, if the reset code (having the encryption code) received matches the reset code stored in the theft

prevention tag, the tag enters a reset mode in which the alarm is disabled. -344 Pet. 43–44 (citing -344 Ex. 1004 ¶¶ 25, 47, 51, 67; -344 Ex. 1017, 57–58). We are persuaded by these contentions. Referring to the operation of the theft prevention tag, Uchida discloses:

> The signal processing unit 5, when the given code is a reset code, determines whether or not the encryption code stored by the encryption storage means 9 and the encryption code included in the cancelation instruction signal match. When the signal processing unit determines that the codes match, the theft prevention tags are set to the reset mode, and when the signal processing unit determines that the codes do not match, the theft prevention tags are set to a warning mode, and a warning signal is output to the drive unit 8.

-344 Ex. 1004 ¶ 51. Uchida describes the "reset mode" as "a state in which an alarm does not output even when detached or when a prescribed signal is received from the transmission device in a state whereby the theft prevention tag is attached to the theft prevention object." -344 Ex. 1004 ¶ 47.

Based on this disclosure, we find Uchida describes these limitations of claims 1 and 22.

e. Determination of unpatentability of claims 1 and 22

For the reasons discussed above, we find Uchida describes all of the limitations of claims 1 and 22. Having considered the full record developed during trial, we determine that claims 1 and 22 are unpatentable under 35 U.S.C. § 102(b) as anticipated by Uchida.

3. Dependent Claims 2–5, 8–11, 13, 15, 16, 18, 21, 23, and 25–29

Petitioner further contends Uchida anticipated dependent claims 2–5, 8–11, 13, 15, 16, 18, 21, 23, and 25–29. -344 Pet. 45–53. Although Patent Owner does not provide specific arguments with respect these claims other

than those presented for the independent claims in this asserted ground of unpatentability, the burden remains on Petitioner to demonstrate unpatentability of all challenged claims. 35 U.S.C. § 316(e); *see also Dynamic Drinkware*, 800 F.3d at 1378. We have analyzed Petitioner's contentions and supporting evidence in light of the limitations recited in dependent claims 2–5, 8–11, 13, 15, 16, 18, 21, 23, and 25–29, and, as explained more fully below with respect to the particular subject matter recited in the dependent claims, we are persuaded Petitioner has demonstrated Uchida anticipated these claims. *See* -344 Pet. 45–53.

a. Dependent claims 2–5

Petitioner contends that Uchida's "conductive wire" that attaches the theft prevention tag to the item of merchandise describes the claimed "attachment cable" that "extends between the security device and the item of merchandise," as recited in claims 2 and 5. -344 Pet. 45–46 (citing -344 Ex. 1004 ¶ 43; -344 Ex. 1017, 58–59). Petitioner further contends Uchida describes that the theft prevention tag alarm sounds in response to cutting or detaching the wire. -344 Pet. 45–46 (citing -344 Ex. 1004 ¶¶ 44, 60; -344 Ex. 1017, 59). We are persuaded by these contentions, and we find Uchida describes the subject matter of these claims. *See* -344 Ex. 1004 ¶ 60 ("[I]f a person attempts to detach the theft prevention tag from the theft prevention object by cutting the conductive wire W . . . , the signal processing unit 5 recognizes the signal thereof through the input part 4, outputs a warning signal to the drive unit 8, and sets the theft prevention tag to alarm mode.").

b. Dependent claims 8 and 9

Petitioner contends Uchida's theft prevention tag and remote control key have LEDs that indicate the status of the respective devices. -344 Pet. 46–47 (citing -344 Ex. 1004 ¶¶ 53, 69; -344 Ex. 1017, 60). We agree, and we find Uchida describes the limitations of these claims. *See* -344 Ex. 1004 ¶¶ 53 (describing that the LED flashes when the theft prevention device alarms), 69 (describing that the LED flashes on the remote control key when the set code or reset code is being transmitted).

c. Dependent claims 10, 16, 21, 23, 25, and 29

With respect to claims 10, 16, 23, and 25, which recite generating or changing the unique security code, Petitioner relies on Uchida's disclosure that the CRS switch on the MRK device is used to change the encryption code. -344 Pet. 47, 49–51 (citing -344 Ex. 1004 ¶¶ 20, 66; -344 Ex. 1017, 60–61, 63, 72). We are persuaded by Petitioner's contentions, and we find Uchida describes the limitations of these claims. *See* -344 Ex. 1004 ¶ 66 ("When the encryption switch (CRS) has been operated, the microcomputer 10 changes the setting of the encryption code included in the reset code to a new encryption code in accordance with the operation.").

We also are persuaded by Petitioner's contention, and we find, that Uchida describes that the logic control circuit stores the unique security code, as recited in claims 21 and 29. -344 Pet. 50, 53 (citing -344 Ex. 1004 ¶ 66, "Explanation of the reference numerals" section; -344 Ex. 1017, 65, 75–76); *see* -344 Ex. 1004, 43 (describing element 10 of the figures as "(4-bit) microcomputer (encryption storage means)").

d. Dependent claim 11

We are persuaded by Petitioner's contention, and we find, that the MRK device describes a "programming station housing the logic control circuit" because microcomputer 10 and other circuitry (i.e., "logic control circuit") are housed within the MRK device. *See* -344 Pet. 47–48 (citing -344 Ex. 1004 ¶ 63, Fig. 3; -344 Ex. 1017, 61).

e. Dependent claim 13

We are persuaded by Petitioner's argument, and we find, that Uchida's disclosure of communication using radio waves describes "the programmable key is configured to wirelessly communicate with the security device," as recited in claim 13. *See* -344 Pet. 48 (citing -344 Ex. 1004 ¶ 67 (describing that the remote control key (RK) "transmits only the set code and reset code to the VS type and WT type theft prevention tag described above using radio waves")).

f. Dependent claim 15

Petitioner contends Uchida's disclosure of the "VS type" theft prevention tag having a switch that activates when detached from the theft prevention object describes "a switch configured to be actuated for activating the alarm in response to the integrity of the security device being compromised." -344 Pet. 48–49 (citing -344 Ex. 1004 ¶¶ 35–36; -344 Ex. 1017, 62–63). Uchida discloses: "If a person attempts to avoid the alarm by detaching the theft prevention tag from the theft prevention object, the button of the theft prevention tag returns, short-circuits the switch VS, and the alarm is also output in this case." -344 Ex. 1004 ¶ 36. We find that the integrity of the security device is compromised when it is detached from the

device it protects without authorization as described. Therefore, we find Uchida describes the subject matter of claim 15.

g. Dependent claim 18

As discussed above with respect to claim 1, Uchida describes "setting a different reset code for each store." -344 Ex. 1004 ¶ 20; -344 Pet. 49–50. Because the reset code (including the encryption code) is different for each store, each store's reset code is "unique" to that store. Therefore, we find Uchida describes the subject matter of claim 18.

h. Dependent claim 26

Petitioner contends Uchida's disclosure of sending a reset code to set the theft prevention device to a reset mode if the codes match describes "disarming the security device upon a matching of the unique security code provided by the logic control circuit with the unique security code stored by the security device." -344 Pet. 51–52 (citing -344 Ex. 1004 ¶ 47; -344 Ex. 1017, 72–74). We are persuaded by these contentions, and we find Uchida describes the subject matter of claim 18 because it discloses, when the codes match, entering a reset mode, "in which an alarm does not output even when detached or when a prescribed signal is received from the transmission device in a state whereby the theft prevention tag is attached to the theft prevention object." -344 Ex. 1004 ¶¶ 47, 51.

i. Dependent claims 27 and 28

Claims 27 and 28 recite communicating and wirelessly communicating, respectively, "the unique security code to the programmable key." We are persuaded by Petitioner's contention that Uchida describes wirelessly communicating (using "radio waves") the encryption code to the

remote control key. -344 Pet. 52–53 (citing -344 Ex. 1004 ¶¶ 66–67; -344 Ex. 1017, 74–75); *see* -344 Ex. 1004 ¶ 63 (describing that the MRK device "transmits the set code, reset code, code that instructs change of operation mode, code that instructs change of VS type/WT type, and encryption code change code that instructs change of the encryption code included in the reset code to the VS type and WT type theft prevention tags described above using radio waves").

j. Determination of unpatentability of dependent claims 2–5, 8–11, 13, 15, 16, 18, 21, 23, and 25–29

In summary, we find Uchida describes the limitations of dependent claims 2–5, 8–11, 13, 15, 16, 18, 21, 23, and 25–29. Having considered the full record developed during trial, we determine that claims 2–5, 8–11, 13, 15, 16, 18, 21, 23, and 25–29 are unpatentable under 35 U.S.C. § 102(b) as anticipated by Uchida.

4. Dependent Claim 19

Claim 19 recites: "The programmable security system of claim 1, wherein the unique security code is not chosen by a person." Petitioner asserts that "Uchida discloses the 'microcomputer 10' changes the 'encryption code' (*i.e.*, unique security code), and the microcomputer is not a person." -344 Pet. 50 (citing -344 Ex. 1004 ¶ 66; -344 Ex. 1017, 64–65). As discussed above, Uchida discloses that, "[w]hen the encryption switch (CRS) has been operated, the microcomputer 10 changes the setting of the encryption code included in the reset code to a new encryption code in accordance with the operation." -344 Ex. 1004 ¶ 66.

Patent Owner argues that this passage from Uchida "references the encryption switch (CRS) being ***operated*** to choose the encryption code, but

it does *not* say whether a person or a computer performs such operation." -344 PO Resp. 28. According to Patent Owner, a different passage from Uchida "discloses that the encryption code is chosen by the 'person in charge.'" -344 PO Resp. 28 (citing -344 Ex. 1004 ¶ 75). In that passage, Uchida discloses: "To change the encryption code included in the reset code, a *person in charge* takes a handy type master remote control key that is usually securely stored in a safe out from the safe, *sets a new encryption code*, and transmits an encryption change code signal." -344 Ex. 1004 ¶ 75 (emphases added). Patent Owner's declarant, Dr. Direen, testifies that the multiple input lines running from the encryption code setting switch (CRS) to microcomputer 10 show "that the CRS encryption switch is composed of multiple switches that are used to manually set the encryption key value" and that "it would have been clear to a [person of ordinary skill in the art] that it is the person in charge that sets the encryption code value via the CRS switches." -344 Ex. 2016 ¶¶ 42–44.

In its Reply, Petitioner disputes Patent Owner's interpretation of Uchida and offers additional testimony from Mr. Allison in support of its positions. -344 Reply 12–13; -344 Ex. 1020 ¶¶ 12–14.

As discussed above with respect to dependent claim 10, we agree with Petitioner that the MRK device generates an encryption code for the system to use. *See* -344 Ex. 1004 ¶ 66 ("When the encryption switch (CRS) has been operated, the microcomputer 10 changes the setting of the encryption code included in the reset code to a new encryption code in accordance with the operation."). Uchida also describes that "a person in charge takes a handy type master remote control key . . . [and] sets a new encryption code." -344 Ex. 1004 ¶ 75. From these passages, it is clear that the MRK device

generates an encryption code for the system, but it is not readily apparent from Uchida the manner in which the encryption code is chosen. Indeed, as noted by Patent Owner (-344 PO Resp. 28), both Petitioner and Mr. Allison assert, with respect to claims 17 and 24, that Uchida "does not disclose how the 'encryption code' is generated." -344 PO Resp. 28 (quoting -344 Pet. 59, -344 Ex. 1017 ¶ 125).

We have considered the evidence before us, and we determine that Petitioner has not shown that Uchida discloses, expressly or inherently, that the encryption code is not chosen by a person.

Petitioner, however, also argues that the additional subject matter recited in claim 19 should be given no patentable weight because the structure of the claimed system "is the same regardless of whether or not the 'security code' is 'chosen by [a] person.'" -344 Reply 6–7. Because we determine that claim 19 is unpatentable under § 103(a) as obvious over the combined teachings of Rothbaum and Denison, we need not separately assess the patentability of this claim under § 102(b). In this case, we do not decide the issue of whether the additional subject matter recited in claim 19 is entitled to patentable weight, and, therefore, we do not reach the ultimate question of whether Uchida anticipated claim 19.

H. Unpatentability Challenge Based on Uchida (§ 103(a) – Claims 17 and 24)

Petitioner asserts claims 17 and 24 would have been obvious based on Uchida. -344 Pet. 9, 58–60. Claims 17 and 24 depend from claims 1 and 23, respectively, and recite generating the unique security code randomly. Petitioner argues that a person of ordinary skill in the art would have been motivated to have microcomputer 10 randomly generate the new encryption

codes because a randomly generated code "provides an extra layer of security" and "because using random numbers is routine in the encryption field, and the code in Uchida is referred to as an 'encryption code.'" -344 Pet. 58–60 (citing -344 Ex. 1004 ¶¶ 65–66; -344 Ex. 1017 ¶¶ 124–128).

Patent Owner argues that using a random number generator does not make sense in Uchida's system, in which there are only 16 possible values for the 4-bit encryption code, because it "would have overcomplicated Uchida's limited 4-bit processing power and resources." -344 PO Resp. 30 (citing -344 Ex. 2016 ¶¶ 46–47). Patent Owner also argues that the odds of repeating a code using a random number generator are higher than if the code is chosen by a person in charge because the person can avoid using recently used codes. -344 PO Resp. 31 (citing -344 Ex. 2016 ¶¶ 49–50). As Petitioner points out, however, having an employee manually enter an encryption code also raises security concerns because "there is a possibility that an employee from one store could provide the code to an unauthorized individual with an MRK" device. -344 Reply 24. Petitioner argues, therefore, that having a code that is randomly generated by the computer and unknown to anyone is more secure than having a code that is manually entered by a person. -344 Reply 24 (citing -344 Ex. 1020 ¶ 47).

We find a person of ordinary skill in the art would have had reason to modify Uchida to have the MRK device randomly generate the encryption codes because doing so would have made them unknown to any person, reducing the risk of an unauthorized person gaining access to the code. -344 Ex. 1020 ¶ 47. Uchida itself describes a benefit in not having the encryption code be known, noting that "since it is complicated to discover the encryption code of the cancelation instruction signal by trial and error, theft

can be further securely prevented." -344 Ex. 1004 ¶ 23. That there are other ways that the code may be chosen merely shows that there were multiple known options available to a person of ordinary skill in the art and does not negate Petitioner's arguments regarding reasons an ordinarily skilled artisan would have had to modify Uchida's system. *See KSR*, 550 U.S. at 421 ("When there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp."). Petitioner has provided sufficient reasoning, supported by the testimony of Mr. Allison and the disclosure of Uchida itself, for why a person of ordinary skill in the art would have been motivated to modify Uchida to randomly generate encryption codes. *See Arendi S.A.R.L. v. Apple Inc.*, 832 F.3d 1355, 1361 (Fed. Cir. 2016) ("[I]n appropriate circumstances, a [claim] can be obvious in light of a single prior art reference if it would have been obvious to modify that reference to arrive at the patented invention.").

Based on the foregoing and having considered the full record developed during trial, we conclude that the subject matter of dependent claims 17 and 24 would have been obvious over Uchida.

I. Unpatentability Challenge Based on Uchida and Garner (§ 103(a) – Claims 6 and 7)

Claim 6 depends from claim 2 and recites that the security system comprises "a recoiler connected to the attachment cable," and claim 7 recites that "the recoiler is located within the security device." Petitioner asserts claims 6 and 7 would have been obvious based on the combination of Uchida and Garner. -344 Pet. 9, 53–55.

Garner discloses using a retractable coil unit in combination with a security tag to hold items together, such as a pair of shoes. -344 Ex. 1005, Abstract, Figs. 1, 2. Figure 1 of Garner is reproduced below.

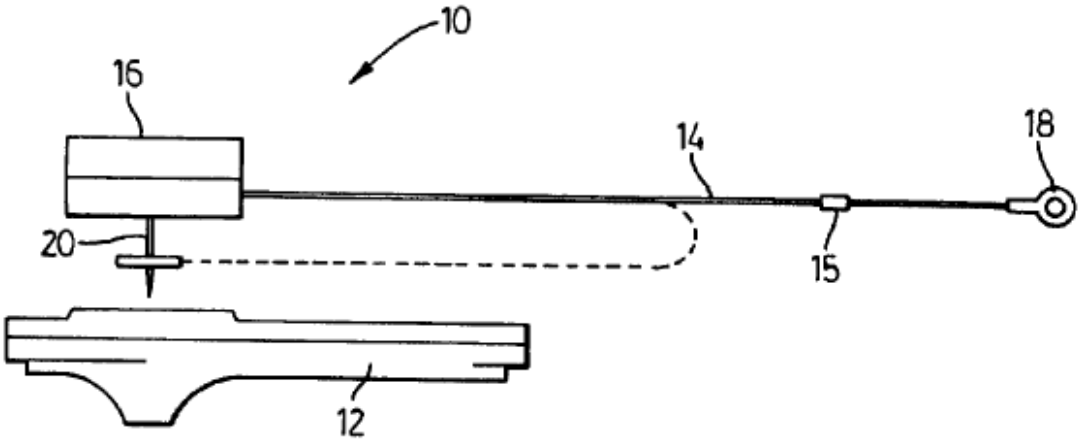


FIG. 1

Figure 1 illustrates "retractable coil unit 10," which "can be locked into the security tag 12." -344 Ex. 1005, 4:14–15. Wire 14 has eyelet 18 through which pin 20 fits and also has stop 15 which keeps wire 14 from fully retracting into coil apparatus 16. *Id.* at 4:15–21.

Petitioner contends:

> A person of ordinary skill in the art ("POSA") would have found it obvious to integrate Garner's "retractable coil unit" (*i.e.*, recoiler) into Uchida's "theft prevention tag." Uchida describes use of a tag with clothing items including shirts with buttonholes. But Uchida's tag modified with Garner's "retractable coil unit" could better protect shoes and other clothing items sold in pairs. A POSA would have found it advantageous to use Garner's "retractable coil unit" because it holds the pair shoes together, but also allows the shoes to be temporarily pulled apart, such that a customer can try them on, as taught by Garner.

-344 Pet. 54 (citing -344 Ex. 1005, 5:3–5; -344 Ex. 1017 ¶¶ 110–112).

We are persuaded that a person of ordinary skill in the art would have found it advantageous to have a recoiler in the security system to allow merchandise to be pulled apart but still held together, as Garner describes. *See* -344 Ex. 1005, 2:14–18, 4:21–5:4; -344 Ex. 1017 ¶¶ 111–112. Garner describes that, with its retractable coil system, "[t]he shoes can be spread apart or retract when returned to display." -344 Ex. 1005, 5:3–4. We credit Mr. Allison's testimony that a person of ordinary skill in the art "would have found it advantageous and desirable to achieve" the functionality of Garner's recoiler within Uchida's system. -344 Ex. 1017 ¶ 112.

Although Patent Owner does not expressly dispute Petitioner's assertion of obviousness with respect to claim 6, which requires that the system "further compris[es] a recoiler connected to the attachment cable," Patent Owner argues Petitioner has not shown that it would have been obvious to have the recoiler "located within the security device," as recited in claim 7. -344 PO Resp. 10–16. Patent Owner argues Garner does not disclose locating the recoiler within security tag 12; rather, according to Patent Owner, this would defeat the purpose of Garner's recoiler because, in Garner, the recoiler is locked into the security device using pin 20 through eyelet 18. -344 PO Resp. 11–13 (citing -344 Ex. 1005, 4:14–18, 5:1–3, Abstract, Figs. 1, 2; -344 Ex. 2014, 53:7–54:11). According to Patent Owner, "if the recoiler were in the tag, the eyelit could not be captured between the recoiler and the tag as provided for in Garner." -344 PO Resp. 16.

In its Reply, Petitioner argues that there are limited options for placement of a recoiler in Uchida's system, including within the housing of Uchida's tag and in a separate housing attached to the tag, and Petitioner

argues both options would have been obvious. -344 Reply 16 (citing -344 Ex. 1020 ¶ 19). Petitioner also argues that both options teach the limitation of claim 7 because "the combination of the tag and 'retractable coil unit' constitutes a security device whether the combination is contained in one housing or two housings attached to each other." -344 Reply 16 (citing -344 Ex. 1020 ¶ 19). Further, Petitioner argues that, even if Garner's security tag 12 were needed, the Uchida-Garner combination, having a recoiler in the theft prevention tag, would still teach the limitations of claim 7. -344 Reply 16 (citing -344 Ex. 1020 ¶¶ 20–21).

We are persuaded by Petitioner's arguments. As Petitioner correctly notes, "Uchida describes use of a tag with clothing items including shirts with buttonholes." -344 Pet. 54. In particular, Uchida describes:

> The theft prevention tag is configured from an IC 1 and an external circuit that is externally attached thereto, and a part of the circuit is short-circuit by a conductive wire that is connected in a state of being attached by being entwined to a button hole or the like of a theft prevention object such as clothing.

-344 Ex. 1004 ¶ 43. Petitioner's argument that "Uchida's tag modified with Garner's 'retractable coil unit' could better protect shoes and other clothing items sold in pairs" (-344 Pet. 54) is supported by the disclosure of Garner, which describes the use of its recoiling wire to protect shoes (-344 Ex. 1005, 5:3–4, Fig. 2).

Patent Owner argues that retractable coil unit 10 includes components coil apparatus 16, pin 20, wire 14, stop 15, and eyelet 18 and that "[o]nly the coil apparatus 16 constitutes the recoiler." -344 PO Resp. 11 (citing -344 Ex. 2014, 53:7–54:11). Patent Owner further argues that "plac[ing] the coil unit 16 ***within*** the security tag 12 would be illogical" because "the disclosed Garner system would ***no longer operate*** due to the absence of the coil unit

16 and pin 20 required to interface with the article of clothing and security tag." -344 PO Resp. 15–16. As discussed above, however, Uchida's theft prevention tag already uses a conductive wire that is looped through merchandise, such as through a buttonhole. -344 Ex. 1004 ¶ 43. We see no impediment to the operation of the Uchida system by including a recoiler in the theft prevention tag to manage the conductive wire of Uchida. We understand Petitioner's contentions to be premised on the use of a recoiler, as taught in Garner, to improve the theft prevention tag of Uchida. *See* -344 Pet. 54; *see also* -344 Reply 16–17 ("[A] separate housing, such as Garner's 'security tag 12,' is not required within the Uchida-Garner combination. Uchida's 'theft prevention tag' with an integrated recoiler is sufficient to protect items of merchandise such as shoes. . . . [T]he 'wire W' of Uchida, attached to the recoiler in the modified system, would easily loop through an eyelet on each of a pair of shoes before being connected to the tag.").

Based on the foregoing and having considered the full record developed during trial, we conclude that the subject matter of dependent claims 6 and 7 would have been obvious over the combined teachings of Uchida and Garner.

J. Unpatentability Challenge Based on Uchida and Burri (§ 103(a) – Claim 12)

Claim 12 depends from independent claim 1 and recites that "the security device comprises a port for receiving the programmable key therein." Petitioner asserts claim 12 would have been obvious based on the combination of Uchida and Burri, on which Petitioner relies for teaching a port for receiving a key. -344 Pet. 55–58.

Figure 1 of Burri is reproduced below.

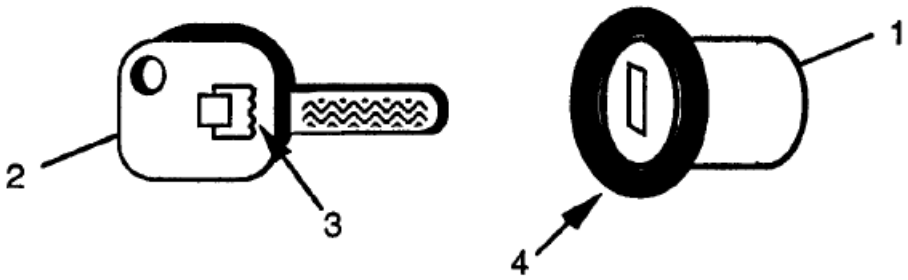


FIG. 1

Figure 1 depicts "an example of an application of the invention in a contactless data transfer system." -344 Ex. 1006, 2:46–47. In Figure 1, key 2 has "a miniature circuit and coil 3 to transfer data by magnetic interaction with the ignition switch, which also has a magnetic coil 4." -344 Ex. 1006, 3:21–24.

Petitioner contends:

> While mechanical interaction is not required for Uchida's communication system to operate (as is also the case in Burri), a [person of ordinary skill in the art] would have been motivated to add a port to Uchida's "theft prevention tag" in order to ensure the proximity required for Uchida's "LC resonance circuit" to function reliably (just as a port is used in Burri). A [person of ordinary skill in the art] would have found it advantageous to use a physical port, as in Burri, for receiving the key, because it would improve the reliability of the data transfer via the "LC resonance circuit" of the Uchida system.

-344 Pet. 57 (citing -344 Ex. 1017 ¶¶ 119–121).

Patent Owner contends Petitioner has not explained sufficiently why a person of ordinary skill in the art would have made the proposed combination. -344 PO Resp. 16–27. In particular, Patent Owner argues that Petitioner is incorrect in asserting that Uchida's system components require proximity to function reliably and that proximity is not required in Uchida

because Uchida's theft prevention tags have power sources and amplifiers to receive radio communications reliably over extended distances. -344 PO Resp. 18–20 (citing -344 Ex. 2016 ¶¶ 15, 18; -344 Ex. 1004, Figs. 1, 2, 4). Patent Owner notes that, by contrast, Burri requires proximity to function because the key is not separately powered but, rather, receives power from the device into which it is inserted. -344 PO Resp. 23 (citing -344 Ex. 1006, 3:45–47, Figs. 1, 2; -344 Ex. 2016 ¶ 26–32). Patent Owner further argues that Uchida describes that its devices use non-contact communication and does not indicate any problem with the reliability of its communication methods. -344 PO Resp. 24 (citing -344 Ex. 1004 ¶ 117, p.3; -344 Ex. 2016 ¶¶ 30–32).

We agree with Patent Owner that Uchida does not describe problems with the reliability of its data communication, but we do not agree that, in Uchida, "proximity is *not* required." -344 PO Resp. 18. As Petitioner points out, Uchida's disarming devices, such as TRK and RK, would have fairly short ranges. -344 Reply 18–19. Uchida discloses:

> A desktop type master remote control key (TRK) is installed at a cash register that is in the vicinity of the exit of the store, and the theft prevention tag (T) is configured to be switched from the set mode to the reset mode from only placing the product on the master remote control key.

-344 Ex. 1004 ¶ 74. Although Petitioner relies on the remote control key (RK) to describe the claimed "programmable key," this disclosure illustrates that proximity is required between components of the system depending on the application. Uchida also discloses that "[t]he remote control key (RK) is used by being formed as a handy type for giving signals to individual theft prevention tags." -344 Ex. 1004 ¶ 68. Because the remote control key (RK) is used to disarm individual tags, we agree with Petitioner that a person of

ordinary skill in the art would understand that the communication range would be small so that other tags in the vicinity would not be accidentally disarmed at the same time as the intended tag. *See* -344 Reply 19 (citing -344 Ex. 1020 ¶ 30).

Patent Owner further argues that "the inclusion of the mechanical ignition key 2 and mechanical ignition switch 1 in Burri is a non-functioning vestige of the particular application of the Burri system—and one that would *not* have been duplicated by a" person of ordinary skill in the art. -344 PO Resp. 25 (citing -344 Ex. 2016 ¶¶ 33–37). The "vestige" to which Patent Owner refers is the insertion of a key into an ignition switch of a car, which, according to Patent Owner, "has no bearing on what a [person of ordinary skill in the art] might have utilized in combination with Uchida." -344 PO Resp. 25–26. Burri is directed to "a data transfer system, particularly, though not exclusively, to a short range contactless data transfer system, and to a demodalator for such a system." -344 Ex. 1006, 1:5–8. Importantly, Burri describes its system for use with a key and a lock and gives an example in the context of an automobile key (-344 Ex. 1006, 3:17–28), which makes it within the field of endeavor of preventing items from theft, as described in the '631 patent (Ex. 1001, 1:26–31). Burri describes the use of ports for receiving keys in systems using short range, non-contact data transmission. -344 Ex. 1006, 1:5–8, 3:17–24. As explained above, Uchida also describes data transmissions of short range between various components of the system. -344 Ex. 1004 ¶¶ 68, 74; -344 Ex. 1020 ¶ 30.

We are persuaded Petitioner has set forth sufficiently articulated reasoning with rational underpinning to support its assertion of obviousness. In particular, the reliability of data transfer is not limited to providing greater

range of communication. Rather, in Uchida's system, it is necessary that only intended tags are disarmed. -344 Ex. 1004 ¶ 68 ("The remote control key (RK) is used by being formed as a handy type for giving signals to individual theft prevention tags."). We are persuaded that having a port on the theft prevention tag into which the key is inserted to disarm the tag would have improved the reliability of the data transfer in Uchida's system by focusing the transmission between two components. *See* -344 Ex. 1017 ¶ 121; Ex. 1020 ¶¶ 30–31. Patent Owner observes that Uchida describes other examples of non-contact communication that could be used, including infrared, and argues that Uchida does not describe problems with the reliability of these communication methods. -344 PO Resp. 24 (citing Ex. 1004 ¶ 117). We agree that Uchida does not describe problems with the reliability of its communication methods, but there is no requirement that a prior art reference identify problems with its own disclosure in order to show that a modification to that reference's disclosure would have been obvious. Rather, "there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *KSR*, 550 U.S. at 418 (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)). Furthermore, as Petitioner points out, for an infrared system, a port would have been beneficial because it would ensure proper line-of-sight alignment between transmitter and receiver. -344 Reply 21–22 (citing -344 Ex. 1020 ¶¶ 37–38). Burri also explains that its system "is not limited to systems using magnetic coupling but is applicable to systems providing energy and data transfer by other contactless means, *such as by light*." -344 Ex. 1006, 7:46–49.

Based on the foregoing and having considered the full record developed during trial, we conclude that the subject matter of dependent claim 12 would have been obvious over the combined teachings of Uchida and Burri.

III. CONCLUSION

Petitioner has demonstrated, by a preponderance of the evidence, that claims 1–29 of the '631 patent are unpatentable.

In particular, Petitioner has demonstrated, by a preponderance of the evidence, that, under 35 U.S.C. § 103(a), claims 1–5, 8–27, and 29 are unpatentable over Rothbaum and Denison, claims 6 and 7 are unpatentable over Rothbaum, Denison, and Ott, and claim 28 is unpatentable over Rothbaum, Denison, and Roatis.

Petitioner also has demonstrated, by a preponderance of the evidence, that claims 1–5, 8–11, 13, 15, 16, 18, 21–23, and 25–29 are unpatentable under 35 U.S.C. § 102(b) as anticipated by Uchida.

Petitioner also has demonstrated, by a preponderance of the evidence, that, under 35 U.S.C. § 103(a), claims 17 and 24 are unpatentable over Uchida, claims 6 and 7 are unpatentable over Uchida and Garner, and claim 12 is unpatentable over Uchida and Burri.

In light of our determination of unpatentability of claim 19 over Rothbaum and Denison under 35 U.S.C. § 103(a), we decline to address whether claim 19 is unpatentable under 35 U.S.C. § 102(b) as anticipated by Uchida.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–29 of the ’631 patent have been shown to be unpatentable.

This is a final decision. Parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

PETITIONER:

Alan H. Norman
Anthony F. Blum
THOMPSON COBURN
anorman@thompsoncoburn.com
ablum@thompsoncoburn.com

PATENT OWNER:

Gregory J. Carlin
David S. Moreland
MEUNIER CARLIN & CURFMAN LLC
gcarlin@mcciplaw.com
dmoreland@mcciplaw.com

Trent A. Kirk
INVUE SECURITY PRODUCTS INC.
trentkirk@invue.com