Trials@uspto.gov
571.272.7822

Paper No. 35
Entered: October 12, 2017

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 IPR2016-00895 and IPR2016-00896
Patent 9,135,800 B2

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

WHITE, *Administrative Patent Judge.*

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

I. INTRODUCTION

A. Background

Mobile Tech, Inc. ("Petitioner") filed two Corrected Petitions seeking to institute *inter partes* review of claims 1–49 of U.S. Patent No. 9,135,800 B2 (Ex. 1001,[1] "the '800 patent") pursuant to 35 U.S.C. §§ 311–319, in Cases IPR2016-00895 and IPR2016-00896. InVue Security Products Inc. ("Patent Owner") filed a Preliminary Response in each proceeding (IPR2016-00895, Paper 8; IPR2016-00896, Paper 8). Based on our review of these submissions, we instituted *inter partes* review of claims 1–49 of the '800 patent. Patent Owner filed a Patent Owner Response and Petitioner filed a Reply in each proceeding, as listed in the following chart.

Case Number	Challenged Claims	Corrected Petition	Decision on Institution	Response	Reply
IPR2016-00895	1–34	Paper 4 ("895 Pet.")	Paper 9 ("895 Dec. on Inst.")	Paper 18 ("895 PO Resp.")	Paper 24 ("895 Reply")
IPR2016-00896	35–49	Paper 4 ("896 Pet.")	Paper 9 ("896 Dec. on Inst.")	Paper 18 ("896 PO Resp.")	Paper 22 ("896 Reply")

Patent Owner does not seek to amend its challenged claims under 37 C.F.R. § 42.121.

[1] Unless otherwise specified with the prefix "896 IPR," we refer to papers and exhibits filed in Case IPR2016-00895.

Patent Owner filed Motions to Exclude certain evidence submitted by Petitioner, Petitioner filed Oppositions, and Patent Owner filed Replies in each proceeding, as listed in the following chart.

Case Number	Motion	Opposition	Reply
IPR2016-00895	Paper 28 ("895 Mot.")	Paper 31 ("895 Opp.")	Paper 32
IPR2016-00896	Paper 26	Paper 28	Paper 29

A combined oral hearing with Cases IPR2016-00892, IPR2016-00898, and IPR2016-00899 was held on June 14, 2017, and a transcript of the hearing is included in the record (Paper 34, "Tr.").

Cases IPR2016-00895 and IPR2016-00896 involve the same challenged patent and parties, and there is overlap in the asserted prior art and other evidence submitted by the parties. To administer the proceedings more efficiently, we exercise our authority under 37 CFR § 42.122 and in accordance with 35 U.S.C. § 315(d) to consolidate the two proceedings for purposes of issuing one final written decision.

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 1–30 and 32–49 of the '800 patent are unpatentable and that Petitioner has not shown, by a preponderance of the evidence, that claim 31 is unpatentable.

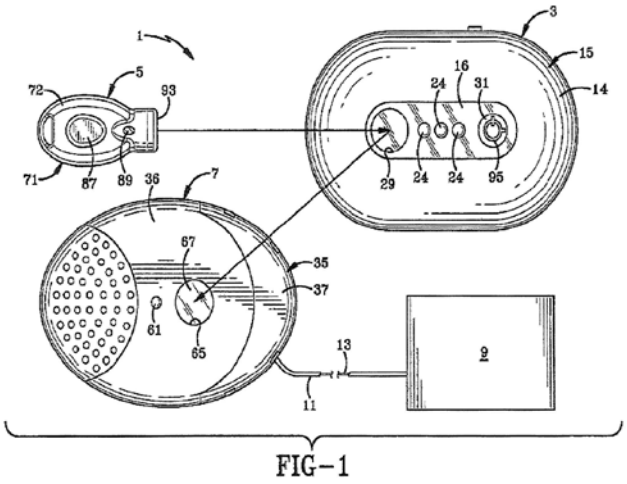
B. Related Proceedings

Petitioner informs us *InVue Security Products Inc. v. Mobile Tech, Inc.*, 3:15-cv-00610 (W.D.N.C.) may be impacted by this proceeding. 895 Pet. 1. In addition, Petitioner filed petitions for *inter partes* review

involving the same parties and related patents. *Id.*; Papers 7, 13, 23; IPR2016-00892, IPR2016-00898, IPR2016-00899, IPR2016-01241, IPR2016-01915, IPR2017-00344, IPR2017-00345, IPR2017-01900, and IPR2017-01901. Also, the parties identify certain patents and pending patent applications that may be impacted by this proceeding. *See id.*

C. The '800 Patent

The '800 patent describes a security system and method including a programmable key. Ex. 1001, 1:23–27. This security system is depicted in Figure 1, which is reproduced below.



FIG–1

Figure 1 depicts security system 1. *Id.* at 6:4–6. The primary components of security system 1 are programming station 3, programmable key 5, and alarm module 7. *Id.* at 6:6–9. Merchandise 9 is connected to alarm module 7 via cable 11 that preferably contains sense loop 13. *Id.* at 6:9–10. Programming station 3 randomly generates a unique security code (Security Disarm Code, or "SDC") that is transmitted to programmable key 5, which in turn stores the SDC in key memory. *Id.* at 9:7–13. Once programmed with an SDC, key 5 is taken to alarm module 7 and the SDC is stored in the alarm module's memory. *Id.* at 9:26–35.

Cable 11 extends between alarm module 7 and item of merchandise 9. 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 and/or causes LED 61 to emit a predetermined flashing pattern. *Id.* at 7:52–64. 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 10:47–59. Programmable key 5 may then be used to re-arm the alarm module. *Id.* at 10:59–61. To disarm and re-arm alarm module 7, the SDC memory of the alarm module must read the same SDC that was generated randomly by programming station 3 and programmed into key 5. *Id.* at 10:59–11:8.

D. Illustrative Claim

As noted above, we instituted review of claims 1–49 of the '800 patent, of which claims 1, 35,[2] 39, and 46 are independent. Claim 1 is illustrative of the challenged claims and is reproduced below:

> 1. A programmable security system for protecting items of merchandise from theft, the programmable security system comprising:
>
> a programming station configured to randomly generate a single security code and having a memory for storing the single security code, the single security code being unique to the programming station;

[2] Claim 35 was corrected in a Certificate of Correction dated February 9, 2016.

a programmable key configured to communicate with the programming station to receive and store the single security code in a memory; and

a security device comprising an alarm and a memory for storing the single security code, the security device configured to be attached to an item of merchandise, the security device further configured to activate the alarm in response to the integrity of the security device being compromised,

wherein the programmable key is configured to arm or disarm the security device upon a matching of the single security code stored in the memory of the security device with the single security code stored by the programmable key.

E. Instituted Grounds of Unpatentability

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

Reference(s)	Basis	Claim(s)
Rothbaum[3] and Denison[4]	§ 103	1, 3–22, and 24–49
Rothbaum, Denison, and Ott[5]	§ 103	2 and 23
Belden[6]	§ 102	1, 3–7, 9–29, and 31–49
Belden and Sedon[7]	§ 103	2
Belden and Rothbaum	§ 103	8
Belden	§ 103	30

[3] U.S. Patent 5,543,782, issued Aug. 6, 1996 ("Rothbaum," Ex. 1005).

[4] U.S. Patent Pub. 2004/0201449 A1, pub. Oct. 14, 2004 ("Denison," Ex. 1003).

[5] U.S. Patent No. 6,380,855 B1, issued Apr. 30, 2002 ("Ott," Ex. 1006).

[6] U.S. Patent Pub. 2007/0159328 A1, pub. July 12, 2007 ("Belden," Ex. 1002).

[7] U.S. Patent Pub. 2005/0073413 A1, pub. Apr. 7, 2005 ("Sedon," Ex. 1004).

II. CLAIM CONSTRUCTION

In an *inter partes* review, "[a] claim in an unexpired patent shall be given its broadest reasonable construction in light of the specification of the patent in which it appears." 37 C.F.R. § 42.100(b). Under this standard, we construe 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 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).

A. Programmable Key"

In the Decisions on Institution, the panel preliminarily determined that the claim term "programmable key" is not "limited to a programmable key that 'deactivates itself upon the occurrence of a specific event,' as argued by Petitioner." *See* 895 Dec. on Inst. 7; 896 Dec. on Inst. 7. The parties do not

dispute this interpretation, and we do not perceive any reason or evidence that compels any deviation from the interpretation. We adopt the previous analysis and need not further interpret the term for purposes of this Decision.

B. "Security Code Is Unique" / "Security Code Being Unique to the Programming Station"

In the Decision on Institution, the panel determined that "a randomly generated security code is within the broadest reasonable interpretation of" the "unique" limitations recited in claims 1, 31, 34, 37–39, and 46–48. *See* 895 Dec. on Inst. 6–7; 896 Dec. on Inst. 6. Claims 1, 39, and 46 recite a security code "being unique to the programming station." Claims 33, 38, and 47 recite that the security code "is unique to a particular retail establishment." Claims 34, 37, and 48 recite that the security code "is unique to a particular retail store."

Patent Owner asserts that the phrase "unique to the programming station" should be given its "[p]lain meaning affording adequate weight to [the] requirement of 'unique' in the context of 'to the programming station.'" 895 PO Resp. 4; *see* 896 PO Resp. 4. According to Patent Owner, "[a]lthough some randomly generated codes are unique, not all randomly generated codes are unique." 895 PO Resp. 5. In support of its position, Patent Owner cites portions of the Specification, claims 42 and 49, and the testimony of Petitioner's Declarant, Thaine Allison III. *Id.* at 4–6.

We are persuaded that, given its broadest reasonable interpretation in light of the Specification, the "unique" phrases in claims 1, 33, 34, 37–39, and 46–48 encompass a randomly generated security code. In multiple places, the Specification characterizes a randomly generated security code as "unique." *See* Ex. 1001, 9:7–13 ("Actuation of activation switch 85 causes

logic control circuit 18 of programming station 3 to randomly generate a unique security code (i.e. SDC) . . . .”), 9:19–23 (“In accordance with one of the objectives and features of the present invention, the SDC initially provided by programming station 3 is randomly generated and is unique to that programming station and always remains with that programming station for subsequent use.”),12:33–39 (“the programmable key . . . is programmed with a randomly generated SDC unique to that particular retail store, and the SDC is initially randomly generated by a programming station used only by that particular retail store”), 15:26–28 (“the logic control circuit further comprises an electronic random number generator for producing a unique SDC”). Thus, while there may be other ways to generate security codes, one way to generate a security code unique to the programming station and/or retail store, according to the Specification of the ’800 patent, is to randomly generate the security code. *See id.* at 15:20–26 (stating that the security code “may be a predetermined (i.e. ‘factory preset’) security code, but preferably is a random security code”).

This is confirmed by claims 42 and 49, which depend respectively from claims 39 and 46 and further recite randomly generating the security code. Contrary to Patent Owner’s arguments, the language of these dependent claims indicates that the parent claims encompass within their scope the random generation of a security code in the programming station (as well as potentially other methods of generation), not that these claims require something “more” than random generation. *See* 895 PO Resp. 6.

We also are not persuaded by Patent Owner’s arguments regarding Mr. Allison’s testimony and the potential sample size for generating a security code that is unique to the programming station. *See id.* (citing

Ex. 2010, 178:24–179:23; Ex. 2013 ¶ 47). In the cited excerpt, Mr. Allison was testifying to uniqueness "[i]n an absolute sense," not in the context of the '800 patent. *See* Ex. 2010, 179:19–23; 895 Reply 18. As Petitioner correctly points out, no number (even in a sample size of one to one billion, for example) is "unique in an absolute sense," and the term "unique" must be interpreted in light of the Specification. *See* 895 Reply 18.

Finally, we note that Patent Owner's proposed interpretation is vague and unclear in scope. Patent Owner contends that "adequate weight" must be given to how "unique" is used "in the claimed context," but Patent Owner does not explain in any detail how much weight should be given or provide any logical basis for determining whether a security code is unique to a programming station or retail store. *See* 895 PO Resp. 4, 6. For this reason as well, we are not persuaded by Patent Owner's arguments.

Accordingly, we interpret "security code being unique to the programming station" in claims 1, 39, and 46, "security code is unique to a particular retail establishment" in claims 33, 38, and 47, and "security code is unique to a particular retail store" in claims 34, 37, and 48 as encompassing (but not being limited to) a randomly generated security code. We need not further interpret the claim language for purposes of this Decision.

C. "Single Security Code"

Claim 1 recites, in relevant part, "a programming station configured to randomly generate a single security code and having a memory for storing the single security code, the single security code being unique to the programming station." Patent Owner asserts that the phrase "single security code" should be construed to mean that a "[p]rogramming station cannot

generate more than one security code for use at a time." 895 PO Resp. 7. Patent Owner contends that "the term 'single' was not separately addressed from the term 'unique' in the Decision to Institute," and, based on the full record, Patent Owner now argues that the term "single" needs to be construed expressly. *Id.* Petitioner asserts that Patent Owner's construction is incorrect because the "single" limitation is not a negative limitation expressing what the programming station cannot do; instead it "requires the programming station be capable of generating a lone security code." 895 Reply 19.

We agree with Patent Owner's assertion that single and unique are separate limitations. The term unique speaks to the difference between codes in a particular context, such as in the context of being unique to a programming station or retail store. The term single speaks to the number of such codes. For example, if different retail establishments used the same code, this could be described as using a single code, but that single code would not be unique to a particular retail establishment. The crux of the dispute between the parties comes down to whether the term single means one or means incapable of more than one. In other words, if a recited programming station generates a "single security code," does that mean that the recited programming station generates a code and also that the programming station is incapable of generating any other code? We are persuaded that the term is not drawn so narrowly as to render the programming station incapable of generating other security codes.

As support for its position, Patent Owner directs us to a passage from U.S. Patent No. 7,737,846 B2 ("the '846 patent," Ex. 2015), which has been incorporated by reference in the '800 patent. *See* 895 PO Resp. 9 (citing Ex.

1001, 1:15–18). The cited passage discusses a feature of the '846 patent, which requires that a smart key be reprogrammed within a specified time period by authorized personnel "in the store having the programmable station and the single unique SDC for all of the security devices in the store." *Id.* (citing Ex. 2015, 2:29–35) (emphasis omitted). Patent Owner appears to be arguing that this passage limits the term "single" such that the programming station is incapable of generating other codes because this passage states that there is a single SDC for all of the security devices in the store. We do not agree. This passage discusses one aspect of the '846 patent, and we do not read this language as limiting the claims of the '800 patent to this one embodiment disclosed in the '846 patent. We see no disclosure that would limit the claimed system such that it could not be used to generate a single security code, for example in a hardware department, and then also be used to generate a single security code, for example for use in an electronics department, at another point in time.

This view comports with Figures 12A and 12B of the '800 patent. *See* 895 Reply 20. According to Petitioner, the figures show a programming station that programs a key with an SDC and then the programming station is reset with a Magic Key thereby allowing the programming station to program another key with another SDC. *Id.* Patent Owner asserts that these figures are irrelevant to Petitioner's argument because they show that there can only be a single SDC active at any one time. Tr. 102:18–103:9. We do not agree with Patent Owner's interpretation of these figures. Petitioner asserts that Figures 12A and 12B illustrate that the "programming station of the preferred embodiment is capable of generating multiple security codes and capable of maintaining a system with multiple keys having different

security codes operating different security devices." 895 Reply 20. Patent Owner's Declarant, Christopher Fawcett, testified that the programming device could be used serially to program two different keys with two different SDCs. Ex. 1017, 146:14–19, 148:25–151:11. Fawcett went on to explain that the first key would no longer be part of the recited system because that key would not be supported by the programming station. *Id.* at 151:3–11. We agree with Petitioner's explanation of the figures and their application to the term "single." Figures 12A and 12B support Petitioner's assertion that the term "single" does not mean that the programming station is incapable of generating more than one security code because, as explained above, the programming station can be used to program multiple keys with multiple SDCs. We are persuaded that the term "single" means one, but it does not limit the programming station such that it is incapable of generating another code.

Accordingly, we interpret "single security code" as one security code, but the recited system does not exclude programming stations that are capable of programming other codes into other keys. We need not further interpret the claim language for purposes of this Decision.

D. "Upon a Matching"

Independent claim 1 recites that "the programmable key is configured to arm or disarm the security device *upon a matching* of the single security code stored in the memory of the security device with the single security code stored by the programmable key." (Emphasis added). In addition, independent claims 35, 39, and 46 each contain similar language reciting that the arming or disarming of the security device occurs "upon a matching."

Patent Owner argues in its Responses that "upon a matching" should be interpreted to mean "on or after a match." 895 PO Resp. 11–18. Petitioner argues that the phrase means "as a result of a determination of a match." 895 Reply 5–10. During the hearing, Patent Owner agreed to the "as a result of" portion of Petitioner's proposed interpretation but disagreed as to the "determination of a match" aspect. Tr. 43:13–45:5, 50:18–21 ("[W]e do agree that there has to be a cause, causal connection. So we would also be happy with, you know, a definition of upon a match being a result of the matching."). Thus, the parties agree that the claim language requires a causal relationship between the matching of the security codes and the arming or disarming of the security devices (i.e., the arming or disarming is "as a result of" the matching). *See id.*; 895 Reply 6. The dispute we must resolve is whether the arming or disarming must be as a result of a "determination of a match." *See* Tr. 86:6–87:19.

We begin with the plain language of the claims. The term "matching" is used as a gerund (i.e., a verb acting as a noun) in each of the independent claims, and ordinarily means "[t]he action of match." Ex. 1020, 4, 6. Thus, the use of "upon a matching" suggests some action of a match, as opposed to, for example, "upon a match," which might be read to require simply the *existence* of a match. This supports Petitioner's view that the arming or disarming must be as a result of a "determination of a match" (a particular type of action).

Turning to the Specification, only the Abstract uses the term "matching," and it largely repeats the phrasing of the claims. Ex. 1001, Abstract. The verb "match" also appears twice. Although this usage is "match" rather than "matching," both times the Specification uses the term

to describe a determination of whether the security code stored in the programmable key is the same as what is stored in the programming station, and then performing some action based on the outcome of that determination. *Id.* at 3:32–37 ("enable the programming station to immediately 'time-out' the key . . . upon the programming station reading a SDC stored in the key that does not match the SDC of the programming station"), 4:4–10 ("the logic control circuit of the programming station may be configured to permanently inactivate the SDC in a programmable key if the SDC programmed in the key does not match the SDC of the programming station"). These portions, therefore, are consistent with Petitioner's proposed interpretation requiring a determination of a match.

The Specification also describes, in connection with disarming and re-arming the security device, reading the security codes in the programmable key and security device to determine if they are the same. "In order to disarm alarm module 7, a programmable key 5 programmed with a valid SDC that is still within the active predetermined time period is placed into the key receiving port 65 of the alarm module, . . . and activation switch 85 is energized by depressing the flexible member 87 on the key." *Id.* at 10:47–52. Alarm module 7 and programmable key 5 then communicate with each other to deactivate the alarm, "thereby enabling cable 11 and any associated sensor to be removed from an item of merchandise 9 for sale of the merchandise to a customer." *Id.* at 10:52–59. "The programmable key 5 may then be used to re-arm the alarm module 7 by again presenting the key to the key receiving port 65 on the alarm module and depressing the flexible member 87 to energize the activation switch 85." *Id.* at 10:59–63.

Importantly, the Specification states that "in order to *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 10:67–11:4 (emphases added). "If a SDC is sensed by alarm module 7 that is *different* than the one stored in SDC memory 53, controller 49 of alarm module 7 will sound alarm 51 to indicate that an invalid programmable key 5 has been used." *Id.* at 11:4–8 (emphasis added); *see also id.* at 4:55–57 ("disarming the security device upon verifying . . . the security code in the alarm module with the security code in the key"). Thus, for disarming and re-arming the security device, the Specification describes reading the security codes in the programmable key and security device and making a determination of whether they match.

Patent Owner acknowledges this disclosure from the Specification with respect to disarming and re-arming but argues that the Specification describes another way to arm "upon a matching." 895 PO Resp. 11–12. According to Patent Owner, programming the security code into the security device "*causes* a ***matching*** of the memories of the programmable key and the security device, thus meeting a condition precedent to arm the device." *Id.* at 13 (first emphasis added). Patent Owner argues that the security codes in the programmable key and security device match "after the programming/storing function occurs" and that "this matching of the SDC codes *must occur* in order to arm the security device," citing the testimony of the parties' declarants and Figure 13 of the '800 patent. *Id.* at 14–15. Petitioner responds that the programming cited by Patent Owner simply involves the security code being "copied from the key into the alarm

module," without any "check . . . to see if the SDC in the alarm module and key 'read the same.'" 895 Reply 9–10. Thus, programming the security device with the security code does not involve "matching" as recited in the claims. *Id.*

We agree with Petitioner as to the initial programming of the security code into the security device. The Specification states that

> [o]nce programmed with the SDC, key 5 is taken to one or more alarm modules 7 (or other security devices) and key end 93 is inserted into key receiving port 65, as shown in FIG. 5. Activation switch 85 of key 5 is then actuated, thereby *programming* the SDC via the communication circuit 50 of alarm module 7 and communication circuit 79 of key 5 into security code (SDC) memory 53 of the logic control circuit 46 of the alarm module 7. SDC memory 53 permanently *stores* the randomly generated SDC in the alarm module 7, preferably for the remaining lifetime of the alarm module.

Ex. 1001, 9:26–35 (emphases added). This merely indicates that the security code is programmed (i.e., stored) into the security device, not that the security device is armed "upon a matching." *See id.*; 895 Reply 8. Indeed, the independent claims separately recite "storing" the security code in the security device and "arm[ing] or disarm[ing]" the security device, indicating that the two actions are not the same. Further, in contrast to the portions of the Specification cited above regarding disarming and re-arming, which specifically refer to the security codes being "read" and being the "same," the portions cited by Patent Owner regarding initial programming include no such language. *See* 895 PO Resp. 13–16 (citing Ex. 1001, 3:67–4:3, 4:45–47, 9:26–39, 11:27–29).

We also are not persuaded by Patent Owner's arguments (*id.* at 15–16) regarding Figure 13 of the '800 patent, which is reproduced below.

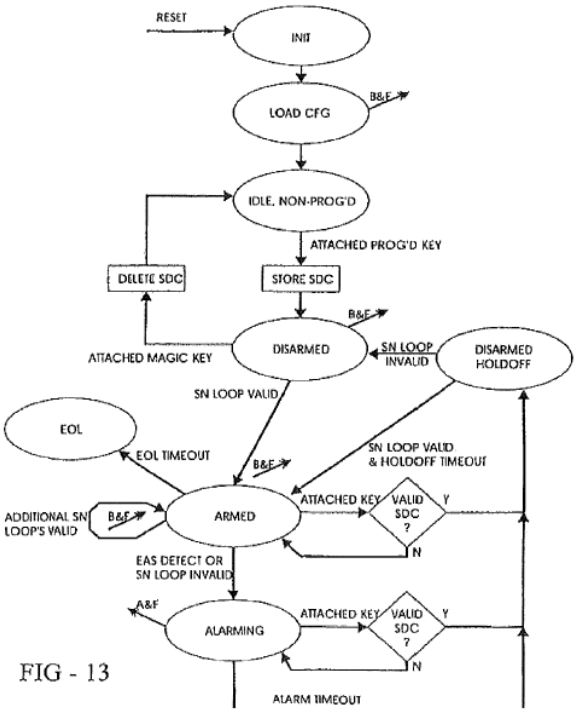


FIG - 13

Figure 13 "illustrates in flow chart form the manner of operation of the logic control circuit 46 of alarm module 7," the sequence of events and actions of which are "readily understood and appreciated by those skilled in the art." Ex. 1001, 11:52–57. Patent Owner contends that "[t]he security device goes from a 'DISARMED' state to an 'ARMED' state *only* upon a matching occurring between the SDC in the programmable key and the code in the security device." 895 PO Resp. 15. The point at which the security codes in the programmable key and security device become the same, however, is earlier—when the security code is first programmed into the security device in the "STORE SDC" step. Ex. 1001, Fig. 13. After doing so, the security device moves to the "DISARMED" state, and only moves to the "ARMED" state when the sense loop connected to the item of merchandise is determined to be valid ("SN LOOP VALID"). *Id.*, Fig. 13, 3:63–4:3; 7:50–8:4. Thus, Figure 13 does not support Patent Owner's position regarding the "upon a matching" claim language.

Finally, we note that the parties also disagree as to whether the "upon a matching" language requires the arming or disarming to take place "immediately" as a result of the matching. *See, e.g.*, 895 PO Resp. 24–25; 895 Reply 6 & n.1; Tr. 44:7–16, 59:9–60:17, 69:19–70:10, 112:11–115:4. Petitioner submits dictionary definitions of "on," including "[o]n the occasion of (an action)," "immediately after (and because of or in reaction to)," and "as a result of." Ex. 1020, 3; *see* 895 Reply 6 n.1 (also arguing that "upon" means "on"). Unlike the disclosure of the Specification cited above, which supports Petitioner's view that the arming or disarming must be "as a result of" a determination of a match, we see no language in the claims or written description pertaining to the timing of when the arming or disarming must occur. Thus, we are not persuaded to read into the claims a requirement that the arming or disarming take place "immediately" after a matching. The only requirement supported by the claim language and Specification is arming or disarming as a result of a determination of a match.

Reading the Specification of the '800 patent as a whole, we are persuaded that Petitioner's proposed interpretation of "upon a matching" is the broadest reasonable interpretation in light of the Specification. Accordingly, we interpret "upon a matching" to mean as a result of a determination of a match.

E. "Configured to Communicate" / "Communicating"

Claims 1 and 46 recite "a programmable key *configured to communicate* with the programming station to receive and store the single security code in a memory" (emphasis added). Claim 39 recites

"*communicating* with the programming station to receive the single security code" (emphasis added).[8]

Petitioner argues that the phrase "configured to communicate" and the term "communicating," as used in the '800 patent, "encompass both wireless and wired forms of communication." *See* 895 Pet. 8; 896 Pet. 8. Petitioner bases this argument on the Specification's disclosure that "[a]nother aspect of the present invention is to provide various forms of data communication between the various elements of the security system," including, "[i]n one preferred embodiment, . . . by wireless communication," and, "[i]n another preferred embodiment, . . . through electrical contacts." Ex. 1001, 3:4–19. Petitioner proposes this interpretation to argue that the application that published as Belden does not describe communication through electrical contacts and, therefore, does not provide written description support for the claimed subject matter reciting "configured to communicate" and "communicating." *See* 895 Pet. 17–19; 896 Pet. 18–20. In particular, Petitioner contends that the continuation-in-part application to which the '800 patent claims priority "broadened the meaning of the term 'communicate' within the claims to encompass the genus of both wireless and non-wireless communication" by reciting other forms of communication, such as communication "through electrical contacts." 895 Pet. 19 (citing Ex. 1001, 3:4–19); *see* 896 Pet. 18–20.

[8] Claim 16, which depends from claim 1, recites that the programmable key is configured to "wirelessly communicate" with the programming station. Claim 40, which depends from claim 39, recites that the communicating step of claim 39 comprises "wirelessly communicating" with the programming station.

We do not agree that the recital of various "forms of data communication" (Ex. 1001, 3:6–21) in the '800 patent broadened the meanings of the phrase "configured to communicate" and the term "communicating." Rather, the "forms" of communication in the cited portion of the '800 patent merely represent examples of the media or means by which the communication occurs in various preferred embodiments. *Id.* (listing at least seven examples, including "wireless communication, such as infrared (IR), radio frequency (RF) or similar wireless communication system[s]," "through electrical contacts," and "induction, for example electromagnetic induction, magnetic induction, electrostatic induction, etc."). Thus, Petitioner does not persuade us that we need to interpret the phrases "configured to communicate" and "communicating" expressly to encompass both wireless and wired communications.

III. ANALYSIS

A. Level of Ordinary Skill in the Art

> Section 103(a) forbids issuance of a patent when "the differences between the subject matter sought to be patented 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) (quoting 35 U.S.C. § 103(a)).

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.

Ex. 1015 ¶ 23. Patent Owner provides a slightly different skill level:

> [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.

895 PO Resp. 18–19 (citing Ex. 2001 ¶ 34). Patent Owner's declarants, Harry Direen, Ph.D., P.E., and Christopher J. Fawcett, testify that a person of ordinary skill in the art would have been

> an engineer (with a B.S. in electrical engineering, computer engineering, computer science, or the equivalent) with 2 to 5 years of experience and trained in electronics including microcontrollers, and embedded programming for microcontrollers. He/she would have been familiar with flowcharts and turning flowcharts and system operational descriptions into working software/firmware. He/she would have been familiar with asynchronous serial communications which were very common in systems that use microcontrollers. He/she would have been adept at turning design concepts into working products.

Ex. 2001 ¶ 34; Ex. 2013 ¶ 39.

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, including the testimony of the parties' declarants, 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.

B. Unpatentability Challenge Based on Rothbaum and Denison

Petitioner asserts that claims 1, 3–22, and 24–49 would have been obvious over the teachings of Rothbaum and Denison. 895 Pet. 33–56; 896 Pet. 32–57. Petitioner provides claim charts in support of its contentions and relies upon the Allison Declaration to support its positions. *Id*.

1. Scope and Content of the Prior Art – 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. Ex. 1005, 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.

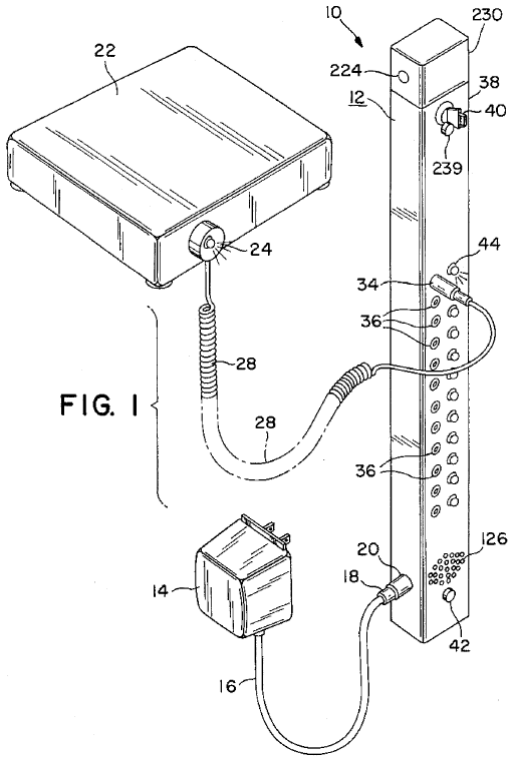


FIG. 1

Figure 1 depicts a perspective view of Rothbaum's security system. *Id.* at 4:22–23. Specifically, it depicts "a twelve jack security system 10 . . . which can protect twelve items of merchandise." *Id.* at 5:10–11. 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; *see id.* at 12:10–18 (describing the activation of an alarm if someone tampers with the security device). "[O]nce 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." *Id.* at 8:23–25.

2. Scope and Content of the Prior Art – Overview of Denison

Denison is directed to vending machines that are equipped with electronic locks. Ex. 1003 ¶ 2. Denison describes vending machines as automated means for selling products. *Id.* ¶ 3. Access to the contents of the vending machine is controlled by an electronic lock and key. *Id.* ¶ 7. In order to unlock the electronic lock, there must be a match between codes stored in the electronic key and electronic lock. *Id.* ¶ 42. Figure 17 of Denison is reproduced below.

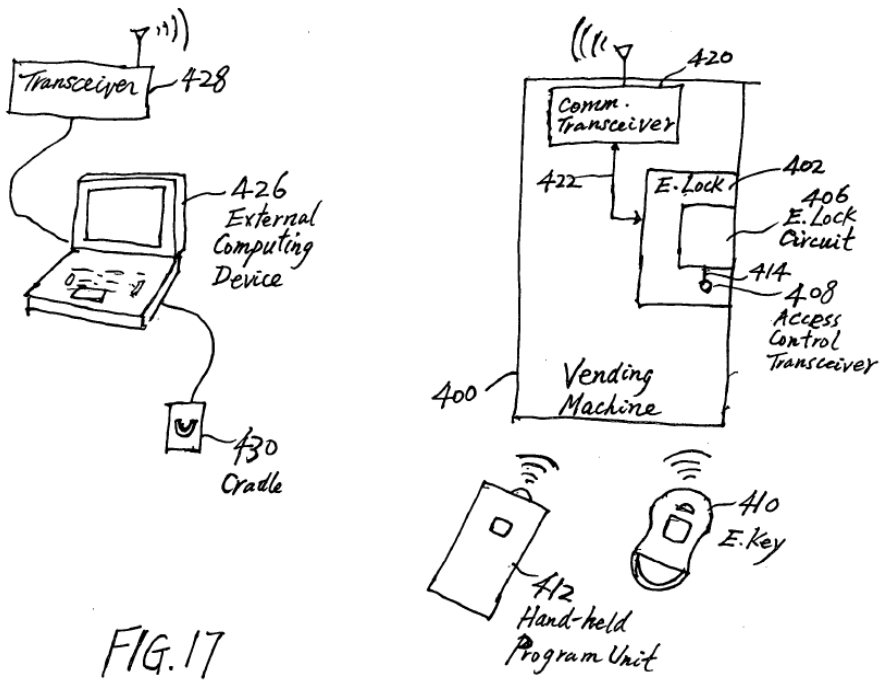


FIG. 17

Figure 17 depicts "a system in which one or more programming schemes may be implemented for field-programming the electronic lock 402 of the vending machine 400 without having to open the vending machine to access a program switch." *Id.* ¶ 77. The vending machine may be opened using electronic key 410, which may be programmed by external computing device 426. *Id.* ¶ 85. External computing device 426 has a memory that

includes an "access code or codes for electronic locks on vending machines, and access control parameters for electronic locks." *Id.* ¶ 79. Database 436 may be resident on external computing device 426. *Id.* "[D]atabase 436 may alternatively or additionally contain programs for computing new access codes and generating control parameters for electronic locks and keys." *Id.* In addition, "external computing device 426 may . . . 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." *Id.* ¶ 84.

In addition, Denison's keys may be limited to operating during certain hours. *Id.* ¶¶ 41, 60. Figure 9 of Denison is reproduced below.

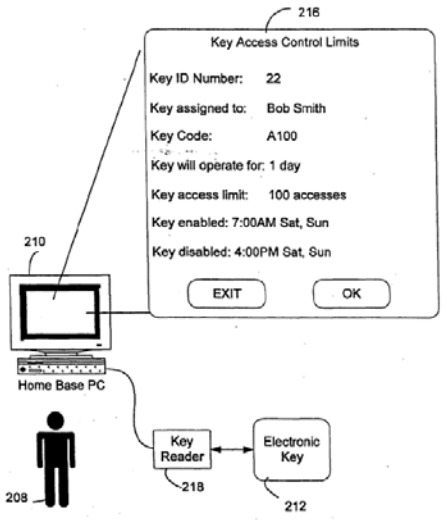


FIG. 9

Figure 9 illustrates a computer used to program operational limits into an electronic key. *Id.* ¶ 23. Operation limits may be customized for each key in the system. *Id.* ¶ 61. These limits could be used to render a key inactive outside of specified work hours. *Id.* A supervisor programs these limits on

a personal computer (PC) and the information is then transferred to the key. *Id.*

3. Analysis of Independent Claims

Independent claims 1, 35, 39, and 46 contain similar limitations and are alleged to be unpatentable as obvious over the teachings of Rothbaum and Denison. 895 Pet. 33–41, 896 Pet. 32–42, 44–50. Petitioner's arguments as to these claims may be summarized as follows: Rothbaum and Denison both describe security systems that protect merchandise from theft. 895 Pet. 39 (citing Ex. 1005, 1:6–9; Ex. 1003 ¶ 6). Petitioner relies upon Rothbaum to teach a security device that is attached to an item of merchandise which causes an alarm when the security device's integrity is compromised. *Id.* at 33–34 (citing Ex. 1005, 1:6–9, 6:15–22, 8:22–38). Denison is relied upon to teach the recited programmable key and programming station through its description of a vending machine with an electronic lock and electronic key wherein external computing device 426 is used to program a key code, which includes an access code, into the memory of the vending machine lock and electronic key. *Id.* at 34 (citing Ex. 1003 ¶¶ 6, 42, 43, 85, 86, Fig. 1.). In addition, Petitioner argues Denison's external computing device generates key codes via its microprocessor and one of ordinary skill in the art would consider this microprocessor to be a logic control circuit, as recited in claim 46 (and claims 32, 45, and 49). 896 Pet. 48 (citing 896 IPR Ex. 1015 ¶ 161[9] pp. 87–88). According to Petitioner, Denison randomly generates an access code, which is part of the "key code." 895 Pet. 38 (citing Ex. 1003 ¶¶ 43, 79, 84). Petitioner argues that Denison

[9] Paragraph 161 continues for nearly thirty pages. Thus, for the purposes of clarity, we identify the page number in addition to the paragraph number.

teaches disarming the security device through its discussion of unlocking the vending machine if the codes stored in the electronic lock and electronic key match. *Id.* (citing Ex. 1003 ¶ 42). Petitioner's Declarant testifies that one of ordinary skill in the art would have understood that Denison's disclosure of changing the inactivating and activating operating limits for an electronic key would teach an electronic key that may be reprogrammed and, thus, by reprogramming a key an inactive key may be reactivated, as recited in claim 35. 896 IPR Ex. 1015 ¶ 161 p. 73.

Petitioner contends that one of ordinary skill in the art would have combined the teachings of Rothbaum and Denison in order to improve Rothbaum's system by replacing its mechanical key with Denison's electronic key. 895 Pet. 35. Petitioner argues that Denison addresses various problems with mechanical locks on vending machines, such as key management and distribution and usage of keys. *Id.* at 34–35 (citing Ex. 1003 ¶¶ 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.

Ex. 1003 ¶¶ 4–5.

Petitioner argues that these problems identified in Denison "would also have been problems present with the security system disclosed in Rothbaum." 895 Pet. 35 (citing Ex. 1015 ¶¶ 172–173). Petitioner's Declarant, Mr. Allison, testifies that

> the 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.

Ex. 1015 ¶ 172.

Petitioner argues that, to address the known problems with mechanical vending machine locks, Denison discloses the use of electronic, field-programmable keys and locks. 895 Pet. 34–35 (citing Ex. 1003 ¶¶ 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.

Ex. 1003 ¶¶ 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." 896 Pet. 35 (citing Ex. 1015 ¶¶ 172–173). 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 alleged invention. 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 36–37 (citing Ex. 1015 ¶¶ 174–178).

We are persuaded by Petitioner's contentions regarding the teachings of Denison and Rothbaum and the motivation to combine these references and find these contentions to be supported by the evidence described above. Patent Owner proffers a number of arguments in opposition to Petitioner's contentions, and we address these arguments below.

a. Rothbaum and Denison are Analogous Art

Patent Owner criticizes the combination of Denison and Rothbaum because "[v]ending machines are not analogous to retail merchandise systems." 895 PO Resp. 34. As part of our obviousness determination, we must assess whether the cited references are 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." 895 Pet. 35 (citing Ex. 1015 ¶¶ 172–173). The '800 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, 1:22–27. Therefore, the '800 patent itself describes the relevant field of endeavor as "protecting merchandise from theft." Further, claims 1, 35, 39, and 46 are directed to programmable security systems 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." Ex. 1005, 1:6–9.[10] Similarly, Denison's disclosure of electronically-locking vending machines is directed to protecting merchandise from theft. *See* Ex. 1003 ¶ 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.").[11] Therefore, both references qualify as prior art to the challenged claims.

---

[10] During oral argument, counsel for Patent Owner acknowledged that Rothbaum is analogous art to the '800 patent. Tr. 94:21–22.

[11] In its Responses, Patent Owner argues that "[v]ending machines are not analogous to retail merchandise systems (using alarms) as [Petitioner] alleges." *See* 895 PO Resp. 34; 896 PO Resp. 35. During oral argument, counsel for Patent Owner stated that "Denison is only somewhat analogous to retail store security" and later clarified that Patent Owner's argument is that Petitioner has not set forth a sufficient rationale to combine the

b. Motivation to Combine Rothbaum and Denison

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. Christopher Fawcett (Ex. 2013), a named inventor on the '800 patent. 895 PO Resp. 33–40. 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 36 (quoting 895 Pet. 35). Patent Owner argues:

> Nothing in Rothbaum . . . teaches or suggests that its mechanical key has any problems. *See* Ex. 2010, 227:23–228:1. Rothbaum's disclosure of a key is very straightforward, generally focusing on the basic functionality of the mechanical key. Ex. 1005 at 6:17–22. Rothbaum at no point mentions problems with such mechanical keys nor does it explicitly or implicitly suggest the mechanical key needs replacing or improvement. Ex. 2013 ¶65.

Id. at 36–37. Mr. Fawcett testifies similarly, citing column 6, lines 17–22 of Rothbaum in his testimony. *See* Ex. 2013 ¶ 65.[12]

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

---

teachings of Rothbaum and Denison, not that Denison is not analogous art to the '800 patent. Tr. 95:11–97:2.

[12] 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* 895 PO Resp. 30–31 (citing Ex. 1005, 6:17–22).

Rothbaum's system, which uses mechanical keys. 895 Pet. 35; Ex. 1015 ¶ 172–173. Indeed, Mr. Allison explains 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." Ex. 1015 ¶ 172. Rothbaum itself discloses that "[o]nly authorized personnel should have access to key 40 to prevent the circumvention of the security system" (Ex. 1005, 6:20–22), underscoring the very security issues identified by Mr. Allison that are encountered in a retail environment. *See* Ex. 1015 ¶ 172. 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. 895 PO Resp. 37–39. With respect to power conservation, Patent Owner argues:

> Rothbaum was also concerned with the need to conserve power in the closed loop system. Ex. 1005, 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. Ex. 2013 ¶67.

Id. at 38. 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 (Ex. 1005, 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 (Ex. 1003 ¶ 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 that

> [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. 2017, 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. 2013 ¶68.

895 PO Resp. 37–38 (alterations in original). 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, Rothbaum's strip or housing 12 is a "security device" as recited in claims 1,

35, 39, and 46. Petitioner does not argue that the programming station 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 too much 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." *Id.* at 37 (citing Ex. 1005, 2:1–6; Ex. 2013 ¶ 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* Ex. 1003 ¶¶ 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 the electronic key system of Denison with the security system of Rothbaum" (*see* Ex. 1015 ¶¶ 174–178) 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.[13] *See* Ex. 1002 ¶¶ 3–10; *see also* Ex. 1001, 1:47–54 (the '800 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. 895 PO Resp. 39. The Federal Circuit, however, has

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

[13] Although Mr. Fawcett testifies regarding increased complexity of the proposed Rothbaum-Denison system (Ex. 2013 ¶ 66), we do not find testimony from Mr. Fawcett rebutting 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), *cert. denied*, 137 S. Ct. 292 (2016) (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* Ex. 1015 ¶¶ 174–178. Indeed, as Petitioner points out (895 Reply 25–26), both of Patent Owner's declarants, Dr. Direen and Mr. Fawcett, testify that a person of ordinary skill in the art "would have been adept at turning design concepts into working products." *See* Ex. 2001 ¶ 34; Ex. 2013 ¶ 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* 895 Pet. 35–37.

Patent Owner further notes that "[a]ll of the independent claims of the '800 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." 895 PO Resp. 35. 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."[14] *Id.* at 36. Patent Owner, therefore, contends Petitioner fails to provide a sufficient rationale to combine Rothbaum and Denison. *See generally id.* at 33–40.

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* 895 Pet. 35–39. 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* Ex. 1015 ¶¶ 172–173; Ex. 1003 ¶¶ 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." Ex. 1003 ¶ 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,"

[14] Although these arguments may be interpreted as directed to the question of whether Denison is analogous art to the '800 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. Tr. 95:11–97:2.

and that "[c]ustomized access limitations may be 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." Ex. 1015 ¶ 172. Rothbaum itself discloses that "[o]nly authorized personnel should have access to key 40 to prevent the circumvention of the security system" (Ex. 1005, 6:20–22), underscoring the very security issues identified by Mr. Allison that are encountered in a retail environment. *See* Ex. 1015 ¶ 172.

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* Ex. 1015 ¶¶ 174–178. 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.*

c. Single Security Code

All of the independent claims of the '800 patent recite a "single security code." Specifically, claim 1 recites "a programming station configured to randomly generate a single security code." Claims 39 and 46 require that a programming station generate a single security code, and claim 35 recites a single security code being stored in each of a plurality of keys and security devices, and "being the same" for each of the security

devices. Patent Owner asserts that the cited art does not teach this single security code because Denison "does not teach or suggest a programming station that cannot generate more than one security code for use at a time." 895 PO Resp. 40–41 (citing Ex. 2013 ¶ 73). This argument is based on Patent Owner's proposed construction of "single security code," which would have required the programming station to be incapable of generating more than code for use at a time. *See id.* at 7, 41. As discussed above, we are not persuaded that the "single security code" requires the programming station to be incapable of generating other codes. *See supra* § II.C.

Petitioner asserts that "[w]hile Denison does not explicitly discuss whether one or multiple access codes are generated at the same time," one of ordinary skill in the art would have found it obvious to generate a single code at a time and provides the example of a user programming a single key for use with a single security device. 895 Pet. 38. We agree with Petitioner's contention that in such a circumstance the user would generate only one code because there would be no need for additional codes. *See id.* Petitioner further explains that even in a system with multiple security devices, a user would be motivated to generate a single code so as to allow that user to have a single key that could disarm all of the security devices. *Id.*; *see* Ex. 1015 ¶ 183[15] p.76. We are persuaded by Petitioner's arguments and evidence, and we find that a person of ordinary skill in the art would have had reason, and would have been motivated, to use a single security code as claimed.

[15] Paragraph 183 continues for more than twenty-five pages. Thus, for the purposes of clarity, we identify the page number in addition to the paragraph number.

d. Unique to the Programming Station

Claims 1, 39, and 46 each recite that the security code is "unique to the programming station." Patent Owner asserts that Petitioner's contentions are insufficient because Petitioner does not explain how one of ordinary skill in the art would ensure that the code is unique to the programming station. 895 PO Resp. 46. Patent Owner contends that Petitioner "makes no effort to evaluate Denison's six-digit random number within the conditions of the 'external computer' in the context of its combination with Rothbaum." *Id.* Much of Patent Owner's argument is premised on its proposed construction of "unique to the programming station"; however, we do not adopt Patent Owner's proposal. *See supra* § II.B.

Denison teaches that access codes for use with the electronic lock and electronic key are generated by external computing device 426. Ex. 1003 ¶ 79. The computing device "may generate the access codes randomly or based on a function that includes the time as a variable." *Id.* ¶ 84. Petitioner contends that an access code stored within Denison's key code is unique to the programming station. 895 Pet. 54. According to Petitioner, "[b]ecause the access code is randomly generated, different external computing devices will not have that code stored, and thus electronic keys programmed by those other devices will not be able to disarm the vending machine." *Id.* (citing Ex. 1015 ¶ 183 pp. 98–99). We find this to be a persuasive analysis of Denison's teachings. In light of our determination that the phrase "unique to the programming station" encompasses randomly generated codes, we are persuaded by Petitioner's contentions, and, thus, we find that the cited art teaches this limitation.

e. Plurality of Security Devices / Plurality of Programmable Keys

Independent claim 35 recites "a plurality of security devices" and "a plurality of programmable keys."[16] Claim 35 further specifies "the single security code being the same for each of the plurality of security devices." According to Patent Owner, these limitations create a "walled off system that cannot operate with more than one unique security code." 896 PO Resp. 51–52 (citing Ex. 2013 ¶ 96). According to Patent Owner, this "walled off system" stands in contrast to Denison, which allows for the generation and management of multiple security codes. *Id.* at 52. Petitioner contends that "Denison discloses a plurality of programmable keys where 'each electronic key 26 has a key code 88 stored therein,' and the key code is the same across those keys." 896 Pet. 36 (citing Ex. 1003 ¶¶ 41, 42, 58). We find this contention to be supported by the disclosures in the reference. Denison states 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. 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.

[16] Claim 24, which depends from claim 1, similarly recites "a plurality of security devices" and "a plurality of programmable keys." Also, claims 43 and 44, which depend from claim 39, recite "a plurality of programming keys" and "a plurality of security devices," respectively. Patent Owner makes similar arguments for claims 24, 35, 43, and 44. *See* 895 PO Resp. 54–56; 896 PO Resp. 51–53. Although we address primarily claim 35 herein, our analysis applies equally to the same limitations in claims 24, 43, and 44.

Ex. 1003 ¶ 42. Denison further explains that its system "provides a consistent and secure means of data transfer between the key and the lock for a condition where *many keys with the same key code will be expected to communicate with many locks* on different vending machines containing that key code." *Id.* ¶ 58 (emphasis added); *see also id.* ¶ 59 ("there may be many keys containing the same key code, and there may be many vending machines that have 'learned' the same key code"). Although Patent Owner is correct in noting that Denison also discloses the management of multiple codes that may access multiple vending machines, this teaching does not negate or teach away from the reference's disclosure of a plurality of keys and locks that share a single access code. Thus, we are persuaded that the cited art teaches this limitation.

f. Configured to Reactivate

Claim 35 recites, in relevant part, "a programming station configured to reactivate each of the plurality of programmable keys after the predetermined period of time." Patent Owner asserts that Denison does not teach the reactivation of keys due to subsequent activation by the programming station; instead, at most it may be said that Denison's initial programming of the key allows the key to be activated again. 896 PO Resp. 47 (citing Ex. 2013 ¶ 108).

Petitioner responds that claim 35 only "requires the programming station be '***configured*** to reactivate each of the plurality of programmable keys after the predetermined period of time.'" 896 Reply 28 (quoting claim 35). According to Petitioner, this claim language may be met if the programming station causes the key to become inactivated after a predetermined period of time and then reactivated. *Id.* Petitioner argues that

Denison teaches a personal computer for customizing "operation limits," for example, based on an employee's "work schedule" such that the key would only be enabled during certain hours. 896 Pet. 37 (citing Ex. 1003 ¶¶ 41, 60 ("The operation limits include, for example, time of data, date, number of days, number of accesses, number of accesses per day, etc."), 61, Fig. 9 (showing "Key Access Control Limits," where the key is disabled at 4:00 PM on Saturday and enabled again at 7:00 AM on Sunday, and the key is limited to "100 accesses")). Petitioner further explains, with supporting testimony from Mr. Allison, that

> [w]hile Denison discloses the "personal computer" (a.k.a., "home base 210") performing this functionality, a [person of ordinary skill in the art] would have found it obvious to combine the functionalities of the home base and external computing device 426 (*i.e.*, "programming station"). Both devices are computers, communicate with the "electronic key 410" via a "cradle" and with the vending machines "wirelessly" over an "RF channel," and both perform "audit" functions. A [person of ordinary skill in the art] would have been motivated to combine the laptop and home base to reduce redundancies and the number of devices in the system.

Id. at 37–38 (citations omitted); *see* Ex. 1015, 71–73.

Patent Owner contends that Denison's disclosure of the personal computer causing the key to become reactivated at a certain time does not teach the limitation of claim 35 because the alleged reactivation is "only as a result of the initial programming by the computer[, n]ot the computer *re*activating the programmable key after a predetermined period of time." 896 PO Resp. 47 (citing Ex. 2013 ¶ 108). Petitioner, however, is correct in noting that claim 35 simply recites that the programming station is "configured to reactivate" the programmable key. We do not see any requirement that the programmable key physically be brought to the

programming station for reactivation or that the programming station perform some active step at the time of reactivation. Rather, we are persuaded that disabling and re-enabling the electronic key in Denison, such that its operation is "limit[ed]" during the disabled time, teach the inactivation and reactivation recited in claim 35. *See* 896 Pet. 33, 37–38; Ex. 1003 ¶¶ 60–61.

Patent Owner also argues that Denison "fails to disclose anything about the personal computer updating or customizing the limits more than once" and that a person of ordinary skill in the art would have "know[n] that there are security risks associated with allowing changes to be made to operation limits on keys after initial programming." 896 PO Resp. 48. Again, we disagree. Denison discloses that "key operation limits may be set by the supervisor 208 of the employee that uses the electronic key 212 to access vending machines in the field." Ex. 1003 ¶ 61. "The limits for each key may be customized depending on, for instance, the work schedule or habits of the employee to whom the key is given." *Id.* Figure 9 of Denison "shows an exemplary user interface screen 216 for prompting the user 208 to enter the limits." *Id.* It would make little sense to make such a user interface available to the employee's supervisor if the operation limits for a key could only be customized once, as Patent Owner contends. If that were the case, for example, the supervisor could never make any changes when the employee's "work schedule" or "habits" change. *See id.* Further, we agree with Petitioner that any concerns regarding security would be alleviated by the fact that the operation limits are set by the employee's supervisor, who likely would keep the personal computer secure. *See* 896 Reply 29 (citing Ex. 1003 ¶ 61).

g. Conclusions of Obviousness

Thus, for all of the foregoing reasons, we are persuaded by Petitioner's contentions as to all of the limitations of independent claims 1, 35, 39, and 46. We also are persuaded that Petitioner has articulated a reasonable rationale with sufficient factual underpinnings to support its allegations that one of ordinary skill in the art would have been motivated to combine the teachings of these references. Patent Owner does not argue or introduce evidence of objective indicia of nonobviousness. Upon consideration of all the evidence, we conclude that Petitioner has proved by a preponderance of the evidence that claims 1, 35, 39, and 46 would have been obvious over Rothbaum and Denison.

4. Analysis of Dependent Claims

Petitioner contends that dependent claims 3–22, 24–34, 36–38, 40–45, and 47–49 would have been obvious over Rothbaum and Denison. 895 Pet. 33–39, 42–56; 896 Pet. 33–39, 42–56. Although Patent Owner does not make any additional arguments with respect to claims 3–14, 16–19, 21, 22, 25, 27–29, 32, 36, 40–42, 45, and 49, and thereby waived any arguments as to their patentability apart from Patent Owner's arguments addressed above in the context of the independent claims, the burden remains on Petitioner to demonstrate unpatentability of all challenged claims. 35 U.S.C. § 316(e); *see* Paper 10, 3 ("Patent Owner is cautioned that any arguments for patentability not raised in the response will be deemed waived."); IPR896 Paper 10, 3; *Dynamic Drinkware LLC, v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015). We have analyzed Petitioner's contentions and cited evidence, including the supporting testimony of Mr. Allison, and agree with and adopt Petitioner's analysis regarding dependent claims 3–22, 24–

30, 32–34, 36–38, 40–45, and 47–49. *See* 895 Pet. 33–39, 42–56; 896 Pet. 33–39, 42–56; Ex. 1015 ¶ 183 pp. 80–101; IPR 896 Ex. 1015 ¶ 128 pp. 48, 51–53, 56–57. For the reasons explained below, however, we are not persuaded Petitioner has shown unpatentability of claim 31 by a preponderance of the evidence.

In addition to the above discussed arguments regarding limitations found in the independent claims, Patent Owner also makes several arguments regarding dependent claims 15, 20, 24, 26, 30, 31, 33, 34, 37, 38, 43, 44, 47, and 48. We address each of these arguments in turn.[17]

a. Dependent Claim 15

Claim 15 depends from claim 1 and further recites "wherein 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. 895 Pet. 44–45. According to Petitioner, "[b]ecause the 'cradle' provides an interface through which a security code is programmed into the programmable key, a [person of ordinary skill in the art] would understand that the 'cradle' is a 'port.'" *Id.* at 45 (citing Ex. 1015 ¶ 183 pp. 85–86). With respect to the claimed "security device," Petitioner explains, with supporting testimony from Mr. Allison, that

> 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 require line

[17] Patent Owner's arguments regarding claims 24, 43, and 44 were addressed above with respect to claim 35, which recites similar limitations. *See supra* § II.B.3.e.

> 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. Further, 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.

Id. at 45 (citations omitted); *see* Ex. 1003 ¶¶ 9, 37, 77; Ex. 1015 ¶ 183 pp. 85–86.

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. 895 PO Resp. 48–49. 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." *Id.* at 49–50 (citing Ex. 1003 ¶¶ 5, 37; Ex. 2007, 4; Ex. 2008, 3, 9). According to Patent Owner and Mr. Fawcett, a person of ordinary skill in the art would have been "greatly deterred from increasing access to the transceiver and lock of Denison by adding a port 'for receiving the programmable key therein,'" where the port would have been "visually detectable and invite[d] tampering, rather than being hidden behind the buttons." *Id.* at 50 (citing Ex. 2013 ¶¶ 80–82).

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* 895 Pet. 45 (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"); Ex. 1015 ¶ 183 pp. 85–86. 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." Ex. 1003 ¶¶ 9, 37, 77; *see* 895 Pet. 45. Further, Patent Owner's arguments do not address Petitioner's proposed combination, which involves modifying Rothbaum's system to use an electronic lock and key rather than a mechanical lock and key. Unlike the vending machine described in Denison, in Rothbaum's system, "the merchandise is accessible from the outside." *See* 895 Reply 28. 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 15 would have been obvious based on Rothbaum and Denison under 35 U.S.C. § 103(a).

b. Dependent Claim 20

Claim 20 depends from claim 1 and further recites "wherein the programmable key comprises a timer, and wherein the programmable key is configured to be inactivated if the single security code stored by the programmable key is not reprogrammed or refreshed by the programming station within a predetermined period of time." With respect to dependent claim 18, which similarly recites that the programmable key comprises a

"timer" and is configured to be "inactivated" after "a predetermined period of time," Petitioner contends:

> Denison also discloses "operation limits" that can be set for the electronic key such that the key becomes disabled (inactivated) after a "predetermined period of time" (e.g., "number of days") using "a real-time clock integrated circuit (IC) 94 (i.e., "timer").

895 Pet. 46–47 (citing Ex. 1003 ¶¶ 41, 60). In particular, Denison discloses that its electronic key includes "a real-time clock integrated circuit (IC) 94 for generating data indicating the date and time." Ex. 1003 ¶ 41. Denison further 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*.

Id. ¶ 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 a "number of days," which teaches a "predetermined period of time."

Petitioner further contends:

> Claim 20 . . . does not require that the key be reprogrammable or refreshable; rather, it requires that the key is configured to be inactivated if the security code stored in the memory of the programmable key is not reprogrammed or refreshed. In other

> words, the requirements of Claim 20 are met by a programmable key configured to be inactivated after a period of time.

895 Pet. 48.

Patent Owner argues that claim 20 "clearly requires that the single security code, not the limits of operation, be refreshed to prevent inactivation." 895 PO Resp. 51; *see also id.* at 52 ("[C]laim 20 requires that the reprogramming or refreshing occur *within* the period of time"). According to Patent Owner, however, "[a]t no point does [Petitioner] allege, or Denison teach or suggest, refreshing or reprogramming the *key code* in the key." *Id.* at 53.

We do not agree with Patent Owner that claim 20 requires reprogramming or refreshing the key. In the Decision on Institution, the panel explained:

> Claim 20 requires the inactivation of the programmable key if the condition to which Patent Owner refers does not happen "within a predetermined period of time." A condition that is *never* met is one that is not met "within a predetermined period of time," thus satisfying the conditional "if" language of claim 20.

895 Dec. on Inst. 24. Based on the full record at trial and applying the preponderance of evidence standard, we maintain the analysis of claim 20 in the Decision on Institution. Contrary to Patent Owner's arguments, reprogramming and refreshing the key code need not be performed to meet the limitations of claim 20. Rather, the claim requires that the key be configured to be inactivated if certain conditions (reprogramming or refreshing the security code) are not met within a predetermined period of time. Patent Owner appears to concede that Denison does not teach reprogramming or refreshing the access code in the key. *See* 895 PO Resp.

53 ("At no point does [Petitioner] allege, or Denison teach or suggest, refreshing or reprogramming the *key code* in the key.").

We find, therefore, Denison discloses a programmable key that is inactivated if the access code in the key is not reprogrammed or refreshed within a predetermined period of time because Denison does not describe refreshing or reprogramming the access code at all. As such, we are persuaded by Petitioner's contention, and we find that the combination of Rothbaum and Denison teaches the limitations of claim 20.

c. Dependent Claim 26

Claim 26 depends from claim 1 and further recites that "the programmable key is configured to provide the single security code to the security device for storing the single 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." 895 Pet. 52–53 (quoting Ex. 1003 ¶¶ 7, 45).

Patent Owner argues that the passages relied upon by Petitioner are from separate embodiments, citing Denison's prosecution history to show that an electronic lock learning a randomly generated security code from an electronic key was added (in a continuation-in-part application) to the previous disclosure of a lock that learns, from a key, an access code set by the factory. 895 PO Resp. 57–58 & n.10 (citing Exs. 1003, 2007, 2020). Patent Owner asserts that Petitioner improperly relies on "the disclosures of . . . two disparate embodiments and do[es] not address the differences in the embodiments and why they might be combined." *Id.* at 58–59. Further, according to Patent Owner, "Denison discloses long range communication between the external computer as a 'home base' and the vending machine

and lock," which "obviates the need to use the key as an intermediary." *Id.* at 59 (citing Ex. 1003 ¶ 73; Ex. 2013 ¶¶ 100–101).

We disagree. Immediately preceding the first paragraph cited by Petitioner, Denison states that "the 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." Ex. 1003 ¶ 6 (emphases added). We agree with Petitioner that by using "and/or," "Denison discloses a vending machine that can learn the key code from any of these devices," including the electronic key, and, therefore, Petitioner is not relying on separate embodiments of Denison. *See* 895 Reply 29. Similarly, Patent Owner's citation to paragraph 73 of Denison regarding the use of the external computer as a "home base" in one scenario (shown in Figure 15) does not negate Denison's teaching of using the electronic key to program the lock or Petitioner's explanation regarding why and how a person of ordinary skill in the art would have combined the teachings of Rothbaum and Denison. *See* 895 PO Resp. 58–59; 895 Pet. 34–40, 52–53; Ex. 1003 ¶¶ 6–7, 73.

We conclude that Petitioner has shown, by a preponderance of the evidence, that claim 26 would have been obvious based on Rothbaum and Denison under 35 U.S.C. § 103(a).

d. Dependent Claim 30

Claim 30 depends from claim 1 and further recites that "the programmable key is configured to be inactivated if the single security code stored in the memory of the security device does not match the single security code stored by the programmable key." As to this limitation,

Petitioner argues that "it would have been obvious to a [person of ordinary skill in the art] to program the key with 'limits of operation' to inactivate the key if the code in the security device does not match the code in the key." 895 Pet. 53. Petitioner supports this assertion with a citation to Denison's description of programming the key with various "limit registers that contain values chosen by a supervisor to limit the operation of [a] particular key." *Id.* at 54 (quoting Ex. 1003 ¶ 60). Petitioner explains that this would be done to further Denison's objective "to reduce the ill-effect of 'stolen or copied keys' that 'may then be used by an unauthorized person.'" *Id.* at 53–54 (quoting Ex. 1003 ¶ 5); Ex. 1015 ¶ 183 pp. 97–98.

Patent Owner contends that this disclosure fails to teach the limitations of claim 30 because "[n]othing about the limits disclosed by Denison, however, is even remotely related to detecting a mismatch of key access codes." 895 PO Resp. 60. According to Patent Owner, Denison's operation limits are there to "guard against *overuse* of the key by limiting time or number of uses." *Id.* (citing Ex. 1003 ¶ 60). In addition, Patent Owner points out that Denison describes an unauthorized attempt to access merchandise with a key whose code that does not match the code in the lock, and, according to Patent Owner, nowhere in that discussion is there a suggestion of invalidating the key. *Id.* at 60–61 (citing Ex. 1003 ¶ 66). Further, Patent Owner argues Denison's system contemplates a system where a key could contain multiple codes and, thus, it would be undesirable to invalidate a key that could still have several valid codes usable with other locks. *Id.* at 61.

Petitioner responds by noting that a person of ordinary skill in the art "would have been familiar with the common security measure of de-

authorizing users who attempt to exceed the scope of their authorization." 895 Reply 30. Also, the combined Rothbaum-Denison system proposed in this ground would contain a single code, and, thus, Patent Owner's discussion of the undesirability of invalidating keys with other valid codes is irrelevant to the proposed ground because in the proposed ground there is only one valid code. *Id.* We agree with Petitioner's argument that the asserted ground is one in which there is only one valid code.

We are persuaded that that it would have been obvious to modify the operation limits to include invalidating a key due to a code mismatch. Denison's Figure 9 illustrates some examples of the operation limits that may be put in place by a supervisor. These exemplars include the number of times that a key may access the lock, authorized access times, the name of the person assigned to use this particular key, the key identification number, and *the key code itself*. Ex. 1003, Fig. 9 (listing "Key ID Number," "Key assigned to," "Key Code," "Key will operate for," "Key access limit," "Key enabled," and "Key disabled" as "Key Access Control Limits"). This list of limits is non-exclusive and "an electronic key may also be programmed with other types of limits of operation of the key." *Id.* ¶ 60. Denison discloses that, "[i]f the access attempt results in a key code mismatch or if the key is disallowed for access because an operation limit in its limit registers is reached, the access process is terminate[d]." *Id.* ¶ 63. "If any of the limits is exceeded, the key will not transmit the key code to the electronic lock and will terminate the operation." *Id.* ¶ 60. We understand Petitioner's assertion to be that one of ordinary skill in the art would create an operation limit such that a key mismatch would invalidate the key. *See* 895 Pet. 53–54. We are persuaded that it would have been obvious to a person of

ordinary skill in the art to modify the system to allow a supervisor to set a limit to inactivate the key upon a mismatch in the same manner that a supervisor could set a limit as to the number of times a key is allowed to access a lock. *See* Ex. 1015 ¶ 183 pp. 97–98 ("When any of the limits are exceeded, 'the key will not transmit the code to the electronic lock.' Thus, when a 'limit of operation' is exceeded, the electronic key becomes inactivated. In view of the various 'limits of operation' examples provided [in Denison], a [person of ordinary skill in the art] would have found it obvious to program the key with 'limits of operation of the key' to inactivate the key if the code in the security device does not match the code in the key."); Ex. 1003 ¶ 60. Once this limit is exceeded then the key "will terminate operation." *See id.* This is a rational modification of Denison's operation limits, particularly given that the key code itself is listed under "Key Access Control Limits" in Figure 9, and we are persuaded that one of ordinary skill in the art would have been motivated to make such a modification to avoid unauthorized usage of the key. *See id.* at 53–54 (quoting Ex. 1003 ¶ 5); Ex. 1015 ¶ 183 pp. 97–98.

We conclude that Petitioner has shown, by a preponderance of the evidence, that claim 30 would have been obvious based on Rothbaum and Denison under 35 U.S.C. § 103(a).

e. Dependent Claims 33, 34, 37, 38, 47, and 48

Claims 33, and 34 depend from claim 1; claims 37 and 38 depend from claim 35; and claims 47 and 48 depend from claim 46. Each of these claims recites additional limitations regarding the uniqueness of the recited security code. Claims 33, 38, and 47 recite that the "single security code is unique to a particular retail establishment," and, similarly, claims 34, 37, and

48 recite the "single security code is unique to a particular retail store." Patent Owner contends that Petitioner has not established that the cited art teaches the recited uniqueness for each of these dependent claims. 895 PO Resp. 62; 896 PO Resp. 54.

As to claims 33, 34, 37, 38, 47, and 48, Petitioner submits 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 programming station, with other retail establishments. 895 Pet. 55; 896 Pet. 55. Petitioner further argues that because the access code of Denison's external computing device 426 is generated randomly, it is "unique" to the particular retail establishment. 895 Pet. 55; 896 Pet. 55.

We find Petitioner's reasoning and cited evidence to be persuasive. The security code's uniqueness appears to represent little more than what one would expect for a key for a mechanical lock in a security device in a retail store. Rothbaum confirms as much: "Only authorized personnel should have access to key 40 to prevent the circumvention of the security system." Ex. 1005, 6:20–22. Further, the random generation of an access code, with one million different possible outcomes (ranging from zero to 999,999, inclusive), as taught by Denison, teaches that the security (access) code is unique, given our interpretation of the "unique" phrases above. *See supra* § II.B. We conclude that Petitioner has shown, by a preponderance of the evidence, that claims 33, 34, 37, 38, 47, and 48 would have been obvious based on Rothbaum and Denison under 35 U.S.C. § 103(a).

f. Dependent Claim 31

Claim 31 depends from claim 1. Claim 31 further recites "the single security code stored by the programming station is unique such that a programmable key programmed by a different programming station is incapable of arming or disarming the security device."

Petitioner argues that a randomly generated access code as described in Denison would not be able to unlock vending machines programmed by other external computing devices because those other external computing devices would not have the same access code. 895 Pet. 54. In support of this position, Petitioner cites Denison's description of external computing device 426 generating an access code (Ex. 1003 ¶ 84) and Denison's description of the process used to ascertain whether the key's code matches the code stored in the electronic lock (*id.* ¶ 42). Based on these disclosures, Mr. Allison testifies that, "[b]ecause the 'access code' that is stored by the programming station ("external computing device 426") is generated randomly, a programmable key ("electronic key") that is programmed by a different external computing device would not receive the same access code and would be incapable of *disarming* the security device." Ex. 1015 ¶ 183 pp. 98–99 (emphasis added).

Petitioner's contentions and Mr. Allison's testimony, however, do not address all of the limitations of claim 31. Petitioner's contentions only discuss the key's inability to *disarm* a security device and, thus, are incomplete because they do not address the recited inability to *arm* the security device. Claim 31 is different from the other challenged claims in that the other claims recite a key "configured to arm or disarm." Ex. 1001, 27:66–67 (claim 1), 29:12–13 (claim 25), 29:60–61 (claim 35), 30:66–67

(claim 46); *see also* 30:27 (claim 39), 30:33–34 (claim 41) (method claims reciting "arming or disarming the security device"). Those claims are written in the alternative such that they may be met by a programmable key that is configured to perform either arming or disarming. The language of claim 31, however, requires the programmable key to lack the ability to arm or disarm a security device, i.e., it is "incapable of arming or disarming the security device." This negative phrasing means that the recited programmable key must be incapable of both arming and disarming. This is supported by the Specification of the '800 patent, which states

> since the SDC in the programmable key 5 is unique to the particular programming station 3 of the retail store that was used to program the key with the SDC, that key cannot be taken to another retail store having the same type of alarm module 7 and used during the predetermined time period to disarm that alarm module. *The programmable key 5 will not function with the alarm module 7 in the other retail store since that alarm module will have been programmed with a different SDC randomly generated by a different programming station 3.* Thus, programmable key 5 overcomes one of the primary disadvantages of current merchandise security systems that use various types of keys since those keys can always be used at other retail stores having similar types of security devices.

Ex. 1001. 9:55–10:1 (emphasis added). We note that, although this passage specifically mentions that the key cannot disarm a security device programmed by another programming station, the language of the passage is broad in that it states that the key "will not function" with a security device in a different store and touts that this key is an advancement over prior art keys because the prior art keys could "always be used at other retail stores." *Id.* Thus, the '800 patent's programmable key is described as being unable

to perform any function when a user attempts to use the key with a security device programmed with a security code from another programming station.

Petitioner, thus, has not put forth sufficient allegations or evidence as to claim 31 because Petitioner does not address the recited key's inability to arm a security device where the key was programmed by a different programming station. Therefore, Petitioner has not established, by a preponderance of the evidence, that claim 31 would have been obvious over Denison and Rothbaum.

g. Conclusions of Obviousness

Thus, for all of the foregoing reasons, we are persuaded that Petitioner has shown that all of the limitations of dependent claims 3–22, 24–30, 32–34, 36–38, 40–45, and 47–49 are taught or at least suggested by the combined teachings of Rothbaum and Denison. We also are persuaded that Petitioner has articulated a reasonable rationale with sufficient factual underpinnings to support its allegations that one of ordinary skill in the art would have been motivated to combine the teachings of these references. Patent Owner does not argue or introduce evidence of objective indicia of nonobviousness. We are not persuaded by Petitioner's allegations as to claim 31. Upon consideration of all the evidence, we conclude that Petitioner has proved by a preponderance of the evidence that claims 3–22, 24–30, 32–34, 36–38, 40–45, and 47–49 would have been obvious over Rothbaum and Denison, but has not done so as to claim 31.

C. Asserted Obviousness in View of Rothbaum, Denison, and Ott

Petitioner asserts that dependent claims 2 and 23 would have been obvious over the combination of Rothbaum, Denison, and Ott. 895 Pet. 56–58. Petitioner explains how the cited prior art references teach the claimed

subject matter and relies upon the Allison Declaration to support its positions. *Id.*

1. Scope and Content of the Prior Art – Ott

Ott "relates 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." Ex. 1006, 1:5–9. Figure 9 of Ott is reproduced below.

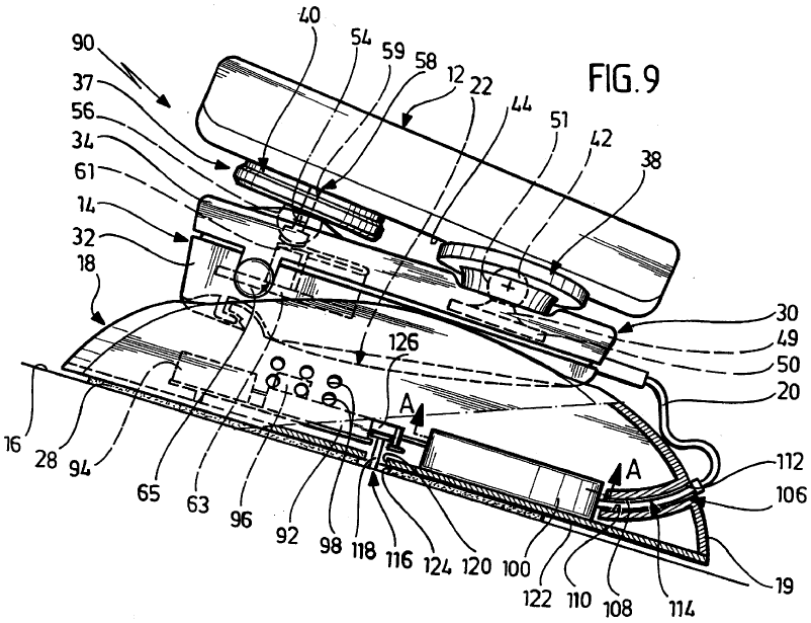


Figure 9 of Ott depicts apparatus 90 having holding part 18 affixed to an object such as lid 16 of a display case and having safeguarding part 14, which can be attached to item of merchandise 12. *Id.* at 7:26–40, 11:43–12:2. Holding part 18 also has sensor element 116. *Id.* at 11:43–57. Ott also discloses switching plunger 118, which actuates microswitch 126 to turn on the alarm when holding part 18 is removed from lid 16. *Id.* at 11:45–12:2.

2. Analysis of Claims 2 and 23

Claim 2 depends from claim1 and further recites "wherein the security device further comprises an adhesive." Claim 23 depends from claims 1, 21, and 22 and further recites "wherein the switch comprises a plunger switch."

As to claim 2, Petitioner argues that

> a [person of ordinary skill in the art] would have been motivated to mount the "strip or housing 12" of Rothbaum onto a supporting structure using "adhesive." Rothbaum discloses the "housing" is "mounted" (*see* Ex. 1005 at 5:23–25), but doesn't specify how. A [person of ordinary skill in the art] would have understood and found obvious that it could be mounted with "adhesive," such as tape. This would have been obvious from the teachings of Ott, or from basic knowledge in the art, including the fact that Rothbaum itself discloses use of "double-backed tape." *See* Ex. 1005 at 5:62–67; *see also* Ex. 1015 ¶¶ 190–192.

895 Pet. 56–57.

We are persuaded by Petitioner's contentions. As an initial matter, we find that Ott is analogous to the claimed invention because Ott describes "an apparatus for safeguarding a merchandise item against theft" (Ex. 1006, 1:5–6) and, therefore, is in the same field of endeavor as the '800 patent, as discussed above with respect to the analogousness of Rothbaum and Denison. *See*, *e.g.*, Ex. 1001, 1:24–29 ("The invention relates to security systems and methods for protecting merchandise from theft . . . ."); *supra* § III.A.2.a.1.

Further, we find that a person of ordinary skill in the art would have had reason, and would have been motivated, to use an adhesive to mount Rothbaum's strip 12 to a supporting structure. *See* Ex. 1015 ¶¶ 190–192. Rothbaum discloses that strip 12 is mounted: "Under normal operation, strip 12 is mounted in a location remote from the merchandise, and preferably

near an AC outlet. Although the strip 12 is shown in a vertical orientation, it may be mounted in any orientation, including horizontally, without affecting its operation." Ex. 1005, 5:21–25. As Petitioner also correctly notes (895 Pet. 57), Rothbaum discloses using an adhesive, such as "double-backed tape," for attaching other items. Ex. 1005, 5:62–67. Ott discloses that "holding part 18 of the apparatus 90 is fixed to the lid 16 by means of the adhesive pad 28, for example by means of a double-sided adhesive tape." Ex. 1006, 11:43–45. Thus, the evidence of record establishes that the use of adhesives for attaching items in security devices was well-known as of the relevant time and that using an adhesive would have resulted predictably in the attachment of two objects (the security device and the support).

We also are persuaded by Petitioner's arguments and evidence as to claim 23. In reference to that claim, Petitioner contends that

> a [person of ordinary skill in the art] would have been motivated to include the "switching plunger" (*i.e.*, "plunger switch") of Ott within and on the bottom of Rothbaum's "housing." *See* Ex. 1006 at 11:45–12:2. Then, the alarm in the "security system" of Rothbaum would also activate if someone removes the housing from its support. This especially would have been obvious given that Rothbaum discloses that its "housing" has anti-tamper capability, including a "tamper switch" to set off the alarm if the "battery compartment" is removed. *See* Ex. 1005 at 12:10–18; *see also* Ex. 1015 ¶¶ 193–94.

895 Pet. 57. We are persuaded that this would be a rational extension of the Rothbaum-Denison combination and that it is supported by sufficient factual underpinnings. As described in Ott, "[a] switching plunger actuates the switching element, with the result that a visual and/or acoustic alarm can be triggered." Ex. 1006, 5:39–41. As explained by Mr. Allison, this modification of "the 'security system' of Rothbaum would also activate if

the entire housing were removed from its supporting structure." Ex. 1015 ¶ 193.

Patent Owner relies on its arguments with respect to the parent claims, and does not argue separately the limitation of claims 2 and 23. *See generally* 895 PO Resp. We conclude that it would have been obvious to use an adhesive to mount strip 12 to a supporting structure in Rothbaum and to use a plunger switch to protect Rothbaum's housing. Based on the foregoing, we determine that Petitioner has shown, by a preponderance of the evidence, that claims 2 and 23 would have been obvious based on Rothbaum, Denison, and Ott under 35 U.S.C. § 103(a). *See* Ex. 1015 ¶¶ 190–194; *see also KSR*, 550 U.S. at 417 ("[W]hen a patent simply arranges old elements with each performing the same function it had been known to perform and yields no more than one would expect from such an arrangement, the combination is obvious." (internal quotation and citation omitted)).

3. Conclusions of Obviousness

Thus, for all of the foregoing reasons, we are persuaded that Petitioner has shown that all of the limitations of claims 2 and 23 are taught or at least suggested by the combined teachings of Rothbaum, Denison, and Ott. We also are persuaded that Petitioner has articulated a reasonable rationale with sufficient factual underpinnings to support its allegations that one of ordinary skill in the art would have been motivated to combine the teachings of these references. Patent Owner does not argue or introduce evidence of objective indicia of nonobviousness. Upon consideration of all the evidence, we conclude that Petitioner has proved by a preponderance of the evidence

that claims 2 and 23 would have been obvious over Rothbaum, Denison, and Ott.

D. Availability of Belden as Prior Art

The '800 patent claims the benefit of priority under 35 U.S.C. § 120 through a chain of applications to an application filed December 14, 2006. Ex. 1001, (63), 1:8–18. The '800 patent also claims the benefit of priority under 35 U.S.C. § 119(e) to a provisional application filed December 23, 2005. *Id.* at (60). The '800 patent in its priority chain contains a "continuation-in-part" application filed June 27, 2011. *Id.* at (63). Petitioner asserts that the challenged claims of the '800 patent are not supported by prior U.S. Patent Application No. 12/770,321, filed April 29, 2010, or by U.S. Patent Application No. 11/639,102, which is the application published July 12, 2007 (Ex. 1002; Belden). 895 Pet. 11–19. Petitioner asserts that because U.S. Patent Application No. 11/639,102 does not provide 35 U.S.C. § 112, first paragraph, support for the challenged claims, the published Belden application constitutes 35 U.S.C. § 102(b) prior art. *Id*. We will refer to Exhibit 1007, which is a copy of U.S. Patent Application No. 11/639,102 as originally filed, as the "'102 application."

1. Legal Principles — Written Description

To comply with the "written description" requirement of 35 U.S.C. § 112, first paragraph, an applicant must "convey with reasonable clarity to those skilled in the art that, as of the filing date sought, he or she was in possession of the invention. The invention is, for purposes of the 'written description' inquiry, whatever is now claimed." *Vas-Cath, Inc. v. Mahurkar*, 935 F.2d 1555, 1563–64 (Fed. Cir. 1991). To "convey with reasonable clarity to those skilled in the art" also may be expressed in terms

of whether the "necessary and only reasonable construction" to be given the disclosure by one skilled in the art clearly supports the limitation now claimed. *See Hyatt v. Boone*, 146 F.3d 1348, 1354 (Fed. Cir. 1998) ("We do not view these various expressions as setting divergent standards for compliance with § 112. In all cases, the purpose 'of the description requirement is to ensure that the inventor had possession, as of the filing date of the application relied on, of the specific subject matter later claimed by him.'") (quoting *In re Edwards*, 568 F.2d 1349, 1351–52 (CCPA 1978)).

One shows "possession" by descriptive means such as words, structures, figures, diagrams, and formulas that fully set forth the claimed invention. *Lockwood v. American Airlines, Inc.*, 107 F.3d 1565, 1572 (Fed. Cir. 1997). "It is not sufficient for purposes of the written description requirement of § 112 that the disclosure, when combined with the knowledge in the art, would lead one to speculate as to modifications that the inventor might have envisioned, but failed to disclose." *Id.*

The invention claimed does not have to be described *in ipsis verbis* to satisfy the written description requirement. *Union Oil Co. v. Atlantic Richfield Co.*, 208 F.3d 989, 1000 (Fed. Cir. 2000). The question of written description support should not be confused, however, with the question of what would have been obvious to the artisan. Whether one skilled in the art would find the claimed invention obvious in view of the disclosure is not an issue in the "written description" inquiry. *In re Barker*, 559 F.2d 588, 593 (CCPA 1977). "A description which renders obvious the invention for which an earlier date is sought is not sufficient." *Lockwood*, 107 F.3d at 1572.

2. Analysis

Petitioner argues that Belden is prior art to the challenged claims because the '102 Application does not provide written description support for two limitations of the challenged claims. *See* 895 Pet. 12–17; 896 Reply 11–20. We begin with these limitations and then proceed to the remaining limitations of the challenged claims.

a. Arming "Upon a Matching"

Petitioner argues that the '102 Application does not provide written description support for the limitation reciting "configured to ***arm*** . . . the security device ***upon a matching*** of the single security code," as recited in claim 1 and similarly recited in claims 35, 39, and 46. *See* 895 Pet. 12–17; 896 Pet. 11–20. We disagree.

The '102 Application includes a number of broad statements that the security device is "controlled" upon a matching of the security codes in the programmable key and security device. For example, claim 1 of the '102 Application recites the "security device being initially programmed with the security code from the key and subsequently being *controlled* by the key *upon matching* the security code of the key with the security code in the security device," and claim 10 includes similar language. Ex. 1007, p. 25, ll. 8–10 (emphases added); *see also id.* at p. 24, ll. 3–6 ("Although the above description refers to the security code being a disarm code, it is understood that the code can activate and *control other functions and features of the security device* such as unlocking the device from the product, shutting off an alarm etc. without departing from the concept of the invention." (emphasis added)), p. 26, l. 22–p. 27, l. 3 (claim 10). These portions do not specifically state that the "control[ling]" can be arming,

however, so we look to other portions of the disclosure to determine the scope of such controlling.

The ’102 Application further discloses:

> In order to disarm alarm module 7, a validly programmed key 5 which is still within its active time period, will be placed into key receiving port 65 as shown in Fig. 5 and switch 85 is energized by depressing on member 87. Wireless communication systems 50 and 79 will deactivate alarm 51 enabling cable 11 to be removed from object 9 or from the alarm module jack 63 for sale of item 9 to a customer or for attachment of a new or different type of merchandise to the alarm module. After the desired product manipulation has occurred, *key 5 is then used to rearm the alarm module*. Again, key LED 90 and alarm module LED 61 will flash in various patterns to indicate that the disarming has occurred and then subsequently that the rearming has occurred.

Id. at p. 18, l. 14–p. 19, l. 1 (emphasis added). Thus, in addition to using the programmable key to disarm the alarm module, the key is “used” to re-arm the alarm module.

Figure 11A (which also appears in the ’800 patent) shows that each time the programmable key is used, it is validated and checked to see if its security code matches the security code stored in the security device. Figure 11A of the ’102 Application is reproduced below.

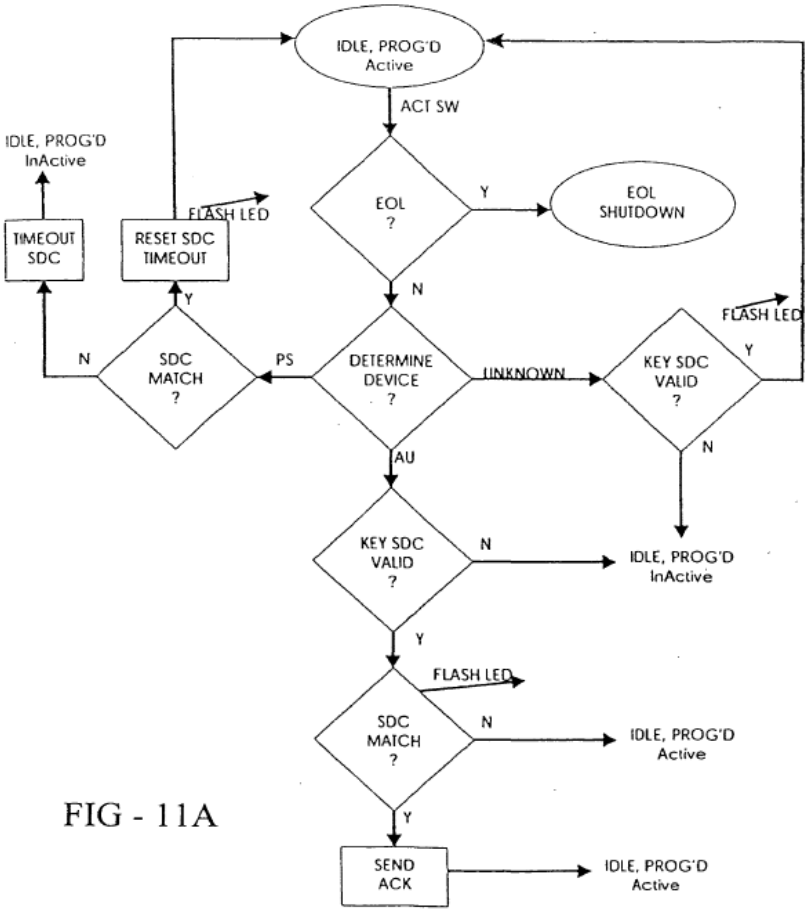


FIG - 11A

Figure 11A depicts "details of the operation of logic control circuitry 77 of programmable key 5," and shows "KEY SDC VALID?" and "SDC MATCH?" steps to determine the validity of the programmable key's security code and whether it matches the security code of the security device, respectively. *See id.* at p. 20, ll. 8–9. Importantly, Petitioner's Declarant, Mr. Allison, agreed that a check is performed for a match of the security codes whenever the programmable key is used. Mr. Allison testified as follows:

> Q. Okay. And is it correct that [Figure] 11A teaches one of skill in the art that a check is done to see if an SDC is in the alarm unit and, if so, if it matches each time the key is used?
>
> MR. NORMAN: Objection. Form.

> A. Yeah. From this flowchart, there's only one arrow for alarm unit, and the first box is "key SDC valid?" with a yes or no.
>
> Q. . . . So that's a "yes"?
>
> A. That's a "yes."
>
> . . .
>
> Q. . . . If a key with an SDC is attached to an alarm module that has a different SDC, the key will not successfully rearm the alarm module because it won't get past the first step because the SDCs don't match?
>
> MR. NORMAN: Objection. Form.
>
> A. Yes. The key will not function in that alarm module.
>
> . . .
>
> Q. Okay. That first step happens whenever the usage of the key is with the alarm module. We already discussed that that first step always happens?
>
> A. Whatever your—one's intent is, *when you place the key into the port of the alarm module, there's a validity check.*
>
> *Q. Okay. Yeah. A comparison of the security code in the key and the security code in the alarm module?*
>
> *A. Yes.*

Ex. 2009, 135:11–20, 139:17–24, 140:24–141:8 (emphasis added).

We agree with Patent Owner and its Declarant, Dr. Direen, that the '102 Application discloses using the programmable key to re-arm the security device, and that such re-arming involves reading the security code from the security device and determining whether it matches the security code of the programmable key. *See* 895 PO Resp. 23, 27–28 & n.9; Ex. 2001 ¶¶ 27–28, 51–55; Ex. 2012 ¶¶ 58, 60–61. Re-arming is simply arming in a particular context (i.e., arming when the security device has been armed previously at least once). *See, e.g.*, Ex. 2009, 91:24–92:7

(Mr. Allison agreeing that "[r]earmed would mean that it had to have been previously armed" and stating that he could not think of "any other differences between armed and rearmed"). We are persuaded, therefore, that the '102 Application provides sufficient written description support for arming the security device upon a matching (i.e., as a result of a determination of a match) of the security codes stored in the programmable key and security device, as recited in the challenged claims.

b. "Configured to Communicate" / "Communicating"

Petitioner also argues, with respect to the "configured to communicate" limitation of claims 1 and 46 and the "communicating" limitation of claim 39, that the '102 Application provides written description support only for wireless communications, whereas the challenged claims allegedly encompass both wireless and wired communications. *See* 895 Pet. 7–8, 17–19; 896 Pet. 8, 18–20.

We do not agree. Claims 1 and 46 of the '800 patent require programmable keys that are "configured to communicate" with the programming station to "receive . . . the single security code." Claims 26 and 29 similarly recite "configured to provide the single security code" to the security device and programmable keys, respectively. Claim 39 recites "communicating with the programming station to receive the single security code." The '102 Application provides express disclosure of this subject matter. For example, the '102 Application describes "ensuring that an active key always has sufficient internal power to receive the SDC and subsequently communicate with the alarm modules for disarming the modules when required." Ex. 1007, p. 4, ll. 13–20. The '102 Application further describes that "[a]nother aspect of the present invention is to enable

the logic control circuit of the programming station to permanently inactivate the SDC in a smart key if the SDC contained therein does not match that of the programming station when in communication with the logic control circuit of the programming station." *Id.* at p. 6, ll. 17–20; *see also id.* at p. 20, ll. 9–12, Fig. 12A (programming station performing the action of "SEND SDC TO KEY"). These two passages demonstrate that the inventors had possession, as of the filing of the '102 Application, of a programmable key that is configured to communicate with the programming station to receive a security code, as recited in the independent claims of the '800 patent.

Petitioner contends that "present invention" statements in the '102 Application limit the scope of the disclosure of the '102 Application to wireless communication only. *See* 895 Pet. 17–19; 895 Reply 12–16; 896 Pet. 18–20; 896 Reply 13–16. In particular, Petitioner argues that the '102 Application "repeatedly limits its scope via 'present invention' statements" and that "[n]owhere does the '102 Application contain a disclosure of non-wireless communication." *See* 895 Pet. 18; 896 Pet. 18–19. We do not agree because, as we find above, the "configured to communicate" and "communicating" limitations of the claims find express written description support in the '102 Application's description of communication between a programming station and programmable key to provide a security code, irrespective of the means by which the communication occurs. *See* Ex. 1007, p. 4, ll. 13–20, p. 6, ll. 17–20.

In support of its "present invention" argument, Petitioner cites, among other cases, *Research Corp. Techs., Inc. v. Microsoft Corp.*, 627 F.3d 859 (Fed. Cir. 2010). According to Petitioner, the Federal Circuit in *Research*

Corp. found that "'the 1990 and 1991 Applications' limited to a 'blue noise mask' via 'present invention' statements could not provide support for the '772 patent, 'which claimed more than the disclosed blue noise mask.'" *See* 895 Reply 12–13, 16; 896 Reply 14, 18. Petitioner's characterization does not tell the whole story. Although the Court stated that "references to 'the present invention' strongly suggest that the claimed invention is limited to a blue noise mask," the Court went on to analyze the full disclosure of the priority applications, stating:

> The specification also explains that the "objects of the invention are accomplished by generating *a blue noise mask* which, when *thresholded at any gray level g, produces a blue noise binary pattern* appropriate for that gray level." Beyond this language, the figures in the patent only illustrate various aspects of a blue noise mask. Finally, all fifteen approved claims of the 1990 Application and all ten approved claims of the 1991 Application recite a "blue noise mask." Accordingly, the 1990 and 1991 Applications disclose only a blue noise mask.

Research Corp., 627 F.3d at 872 (citations omitted). The Court's determination was not based solely on "present invention" statements in the priority documents. Rather, the Court looked to the entire disclosure to determine that the priority applications "disclose only a blue noise mask." *See id.* Similarly, we look to the entire disclosure of the '102 Application, which expressly describes communication between a programming station and programmable key to provide a security code, irrespective of the means by which the communication occurs.[18] *See* Ex. 1007, p. 4, ll. 13–20, p. 6, ll. 17–20.

[18] Indeed, claim 1 of the '102 Application broadly recites "a programming station for generating a security code into the key," and claim 2, which

The pertinent inquiry is whether the '102 Application provides written description support for communication between a programming station and programmable key to provide a security code. For the reasons discussed above, we find that it does. That U.S. Patent Application No. 13/169,968 to which the '800 patent claims priority lists *additional* means or media through which communication takes place does not take away from the express disclosure of the '102 Application.

c. Other Limitations

As explained above, we find that the '102 Application provides sufficient written description support for arming the security device "upon a matching" of the security codes stored in the programmable key and security device, and the "configured to communicate"/"communicating" limitations. With respect to the remaining limitations, Petitioner asserts that Belden anticipates claims 1, 3–7, 9–29, and 31–49. *See* 895 Pet. 11–29; 896 Pet. 11–31. As such, Petitioner does not contend that Belden (the publication of the '102 Application) fails to provide disclosure for the subject matter of these claims other than with respect to arming "upon a matching" and communicating the security code. Patent Owner does not dispute that Belden discloses the other limitations of the claims. We have reviewed the citations provided by Petitioner and are persuaded that the '102 Application (which published as Belden) provides sufficient written description support for claims 1, 3–7, 9–29, and 31–49.

---

depends from claim 1, limited that to a "wireless" interface for generating the security code into the key. Ex. 1007, p. 25, ll. 5–6, 12–13.

d. Conclusion

Based on the record developed during trial, we determine that the '102 Application conveys with reasonable clarity to those skilled in the art that, as of its filing date, the inventors were in possession of the inventions recited in claims 1, 3–7, 9–29, and 31–49 of the '800 patent. Accordingly, these claims are entitled to the benefit of the filing date of the '102 Application (December 14, 2006) and Belden is not prior art to these claims. Petitioner has not shown, by a preponderance of the evidence, that claims 1, 3–7, 9–29, and 31–49 are anticipated by Belden under 35 U.S.C. § 102(b).

F. Obviousness Grounds Based on Belden

Petitioner additionally asserts that claim 2 would have been obvious based on the combination of Belden and Sedon. *See* 895 Pet. 29–31. Petitioner contends that claim 8 would have been obvious over Belden and Rothbaum. *Id.* at 31–32. In addition, Petitioner asserts that Belden alone renders obvious claim 30. *Id.* at 32–33. Because we conclude that claim 2 is unpatentable over the combined teachings of Rothbaum, Denison, and Ott and claims 8 and 30 are unpatentable over the combined teachings of Rothbaum and Denison, we need not separately assess the patentability of claim 2, 8, and 30 based on Belden alone or in combination with Sedon or Rothbaum, and thus need not determine whether Belden is prior art to claims 2, 8, and 30.

IV. MOTION TO EXCLUDE

Patent Owner filed a Motion to Exclude[19] Exhibits 1018, 1019, and 1020, which are dictionary definitions Petitioner cites in support of its construction of the phrase "upon a matching." Patent Owner argues that these exhibits are "irrelevant and prejudicial under [Federal Rules of Evidence] 401 and 403, as well as outside the permissible scope of a reply." 895 Mot. 2. Patent Owner argues Petitioner "provides no justification for why extrinsic evidence can be resorted to in this case, nor why these particular references (and not other dictionary and grammar sources) should control." *Id.*

We are not persuaded Exhibits 1018, 1019, and 1020 should be excluded. *See* 37 C.F.R. § 42.20(c) ("The moving party has the burden of proof to establish that it is entitled to the requested relief."); *see also* 37 C.F.R. § 42.64(c) ("Motion to exclude"). Federal Rule of Evidence 401 provides that "[e]vidence is relevant if: (a) it has any tendency to make a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the action." As Patent Owner acknowledges, Petitioner proffers these exhibits as evidence of the meaning of disputed claim language, specifically the phrase "upon a matching." 895 Mot. 2. The meaning of this phrase is "of consequence in determining" whether or not the '800 patent claims are entitled to the benefit of the

[19] The parties filed substantially similar Motion to Exclude (IPR2016-00896, Paper 26), Opposition (IPR2016-00896, Paper 28), and Reply (IPR2016-00896, Paper 29) in IPR2016-00896. For ease of reference we cite to the papers in IPR2016-00895, but this analysis also applies to the Motion to Exclude in IPR2016-00896.

priority date of the '102 Application and whether they are anticipated or obvious over the asserted prior art, and Exhibits 1018, 1019, and 1020, even if not expressly relied upon in our Decision,[20] provide insight as to the meaning of the phrase "upon a matching." Therefore, we determine Exhibits 1018, 1019, and 1020 have some "tendency to make a fact more or less probable than it would be without the evidence" and are relevant under Federal Rule of Evidence 401.

Federal Rule of Evidence 403 provides that relevant evidence may be excluded "if its probative value is substantially outweighed by a danger of one or more of the following: unfair prejudice, confusing the issues, misleading the jury, undue delay, wasting time, or needlessly presenting cumulative evidence." Patent Owner does not explain in its Motion why any of these factors substantially outweighs the probative value of Exhibits 1018, 1019, and 1020. We find the exhibits relevant and are not persuaded that they should be excluded under Federal Rule of Evidence 403.

We also are not persuaded by Patent Owner's arguments that this evidence should be excluded because it is "outside the permissible scope of a reply" and "should have been presented at the time of filing the petition." 895 Mot. 2–3. A motion to exclude is limited to arguing that material is inadmissible under the Federal Rules of Evidence. *See* 37 C.F.R. §§ 42.62(a), 42.64(c); Office Patent Trial Practice Guide, 77 Fed. Reg. 48,756, 48,767 (Aug. 14, 2012) ("A motion to exclude must explain why the evidence is not admissible (*e.g.*, relevance or hearsay) . . . ."). Even if Patent Owner's arguments were proper procedurally, however, Petitioner

[20] We do not cite Exhibits 1018 and 1019 in our analysis. Nonetheless, we do not exclude this evidence from the record.

introduced this evidence in response to Patent Owner's arguments in its Response as to the meaning of "upon a matching." *See* 895 Opp. 3–4. Specifically, Patent Owner argued that the phrase means "on or after a match," and Petitioner cited the dictionary definitions in support of its argument that Patent Owner's proposal was unreasonably broad because "upon" requires a "causal relationship . . . between the matching of the security codes and the arming or disarming of the security device" (i.e., "the key [is] configured to arm or disarm the security device *as a result of* the matching of the codes").[21] *See* 895 PO Resp. 11–18; 895 Pet. Reply 6 & n.1 (citing Exhibits 1018, 1019, and 1020); 895 Opp. 2–4. Pursuant to 37 C.F.R. § 42.23(b), "[a] reply may only respond to arguments raised in the corresponding . . . patent owner response." We determine Petitioner's Reply arguments, and evidence in support thereof, with respect to the meaning of the phrase "upon a matching" are permissible reply arguments.

In its Motion to Exclude, Patent Owner also "objects to [Petitioner]'s misquotation and limited introduction of transcript testimony from Chris Fawcett (Ex. 1017) and Harry Direen (Ex. 1016)." 895 Mot. 3. Patent Owner identifies various citations in Petitioner's Reply to which Patent Owner objects as misquotations of testimony or citations in incomplete testimony. *Id.* at 3–5. Patent Owner argues that, under Federal Rule of Evidence 106, "statements in the transcript cannot be read out of context of other supporting statements" and that "misquoted or partial testimony should be considered in context with other testimony on the subject or the alleged

[21] As explained above, Patent Owner subsequently agreed with the "as a result of" portion of Petitioner's proposed interpretation during the hearing. *See supra* § II.D; Tr. 43:13–45:5, 50:18–21.

testimony support should be excluded as unsupportive of [Patent Owner]'s positions." *Id.* at 3.

Federal Rule of Evidence 106 provides: "If a party introduces all or part of a writing or recorded statement, an adverse party may require the introduction, at that time, of any other part—or any other writing or recorded statement—that in fairness ought to be considered at the same time." This Rule provides a basis for including, rather than excluding, evidence. In this case, Exhibits 1016 and 1017 are the complete transcripts of the depositions of Dr. Direen and Mr. Fawcett, respectively, and, therefore, the additional portions of Exhibits 1016 and 1017 that Patent Owner cites for our consideration are already part of the record in this matter and have been considered in rendering our Decision. As such, Patent Owner's request for relief under Federal Rule of Evidence 106 is moot.

Based on the foregoing, Patent Owner's Motion to Exclude is denied as to Exhibits 1018, 1019, and 1020 and dismissed as moot as to Exhibits 1016 and 1017.

V. CONCLUSION

Based on the information presented and the record developed during trial, we conclude that Petitioner has shown by a preponderance of the evidence that (1) claims 1, 3–22, 24–30, and 32–49 are unpatentable under 35 U.S.C. § 103(a) as having been obvious over Rothbaum and Denison; and (2) claims 2 and 23 are unpatentable under 35 U.S.C. § 103(a) as having been obvious over Rothbaum, Denison, and Ott. Petitioner, however, has not shown by a preponderance of the evidence that claim 31 is unpatentable over Rothbaum and Denison, or that claims 1, 3–7, 9–29, and 31–49 are unpatentable as anticipated by Belden. In light of our other determinations

of unpatentability, we decline to address whether claim 2 is unpatentable as obvious over Belden and Sedon; whether claim 8 is unpatentable as obvious over Belden and Rothbaum; and whether claim 30 is unpatentable as obvious over Belden.

VI. ORDER

Accordingly, it is:

ORDERED that claims 1–30 and 32–49 of the ’800 patent have been shown to be unpatentable;

FURTHER ORDERED that claim 31 of the ’800 patent has not been shown to be unpatentable;

FURTHER ORDERED that Patent Owner’s Motions to Exclude are *denied-in-part* and *dismissed-in-part*; and

FURTHER ORDERED that, because this is a final written 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 Norman
Anthony Blum
David Jinkins
Matthew Braunel
THOMPSON COBURN LLP

tc-ipr-mti@thompsoncoburn.com
ablum@thompsoncoburn.com
djinkins@thompsoncoburn.com
mbraunel@thompsoncoburn.com

PATENT OWNER:
Gregory Carlin
Warren Thomas
Trent Kirk
MEUNIER CARLIN & CURFMAN LLC
mti.invue.iprs@mcciplaw.com
wthomas@mcciplaw.com
trentkirk@invue.com