

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KINGSTON TECHNOLOGY COMPANY, INC.,
Petitioner,

v.

SPEX TECHNOLOGIES, INC.,
Patent Owner.

Case IPR2017-00825
Patent 6,003,135

Before LYNNE E. PETTIGREW, DANIEL N. FISHMAN, and
CHARLES J. BOUDREAU, *Administrative Patent Judges*.

BOUDREAU, *Administrative Patent Judge*.

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

I. INTRODUCTION

Kingston Technology Company, Inc. (“Petitioner”) filed a Petition requesting *inter partes* review of claims 55 and 57 of U.S. Patent No. 6,003,135 (Ex. 1001, “the ’135 patent”). Paper 2 (“Pet.”). SPEX Technologies, Inc. (“Patent Owner”) filed a Preliminary Response. Paper 7 (“Prelim. Resp.”).

Under 35 U.S.C. § 314, an *inter partes* review may not be instituted “unless . . . there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a). For the reasons that follow, we are not persuaded, on this record, that Petitioner has established a reasonable likelihood of prevailing in showing the unpatentability of any of the challenged claims on the asserted grounds. Accordingly, we *deny* the Petition and decline to institute an *inter partes* review of claims 55 and 57 of the ’135 patent.

II. BACKGROUND

A. *Related Matters*

The parties indicate that the ’135 patent is involved in *SPEX Technologies, Inc. v. Kingston Technology Co. Inc.*, No. 8:16-cv-01790 (C.D. Cal. Filed Sept. 27, 2016); *SPEX Technologies, Inc. v. Western Digital Corp.*, No. 8:16-cv-01799 (C.D. Cal. Filed Sept. 28, 2016); *SPEX Technologies, Inc. v. Toshiba America Electronics Components Inc.*, No. 8:16-cv-01800 (C.D. Cal. Filed Sept. 28, 2016); *SPEX Technologies, Inc. v. CMS Products, Inc.*, No. 8:16-cv-01801 (C.D. Cal. Filed Sept. 28, 2016); *SPEX Technologies, Inc. v. Integral Memory, PLC*, No. 8:16-cv-01805 (C.D. Cal. Filed Sept. 28, 2016); and *SPEX Technologies, Inc. v.*

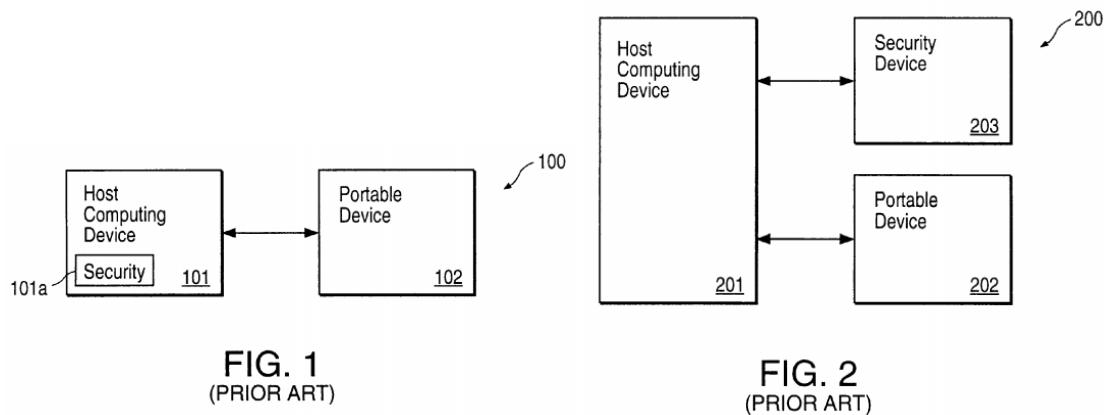
Apricorn, No. 2:16-cv-07349 (C.D. Cal. Filed Sept. 28, 2016). Pet. 2;
Paper 3, 2–3.¹

The '135 patent also is the subject of a petition for *inter partes* review filed March 14, 2017, by Petitioner. Case IPR2017-01021, Paper 2.

B. The '135 Patent

The '135 patent is directed to a modular device that can communicate with a host computing device to enable one or more security operations to be performed by the modular device on data stored within the host computing device, data provided from the host computing device to the modular device, or data retrieved by the host computing device from the modular device.

Ex. 1001, 1:17–26. Figures 1, 2, and 4B of the '135 patent are reproduced below.



¹ We note that Patent Owner's Mandatory Notices Pursuant to 37 C.F.R. § 42.8(a)(2) (Paper 3) does not include page numbers. For ease of reference, the Parties are advised to include page numbers in all filings.

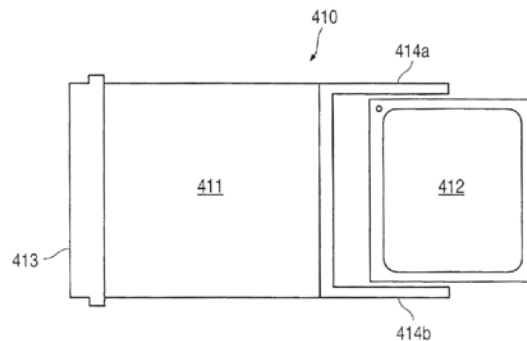


FIG. 4B

Figures 1 and 2 are block diagrams of prior art systems described in the '135 patent. *Id.* at 1:51–3:14, 6:3–8. Figure 4B is a plan view of a modular device according to one embodiment of the invention of the '135 patent. *Id.* at 6:18–20. The '135 patent explains that in the prior art, security operations were either performed by the host computer, as illustrated in Figure 1 with security mechanism 101a included in host computing device 101, or by a standalone security device, as illustrated by security device 203 in Figure 2. *Id.* at 1:57–58, 2:21–31. According to the '135 patent, both of those arrangements were deficient in various ways. *Id.* at 2:9–20, 2:58–3:14. The '135 patent purports to solve those deficiencies by placing a security module between the host and target modules. With reference to Figure 4B reproduced above, the '135 patent explains that either first module 411 or second module 412 can be a security module and the other can be a target module. *Id.* at 8:25–27. The '135 patent further explains, however, that connector 413 makes connection to a host computing device, and it is therefore preferable that first module 411 be the security module and second module 412 be the target module “to facilitate implementation of the in-line security aspect of the invention.” *Id.* at 8:27–32.

C. Challenged Claims

The challenged claims are reproduced below:

55. For use in a modular device adapted for communication with a host computing device, the modular device comprising a security module that is adapted to enable one or more security operations to be performed on data and a target module that is adapted to enable a defined interaction with the host computing device, a method comprising the steps of:

receiving a request from the host computing device for information regarding the type of the modular device;

providing the type of the target module to the host computing device in response to the request; and

operably connecting the security module and/or the target module to the host computing device in response to an instruction from the host computing device.

57. For use in a modular device adapted for communication with a host computing device, the modular device comprising a security module that is adapted to enable one or more security operations to be performed on data and a target module that is adapted to enable a defined interaction with the host computing device, a method comprising the steps of:

communicating with the host computing device to exchange data between the host computing device and the modular device;

performing one or more security operations and the defined interaction on the exchanged data;

mediating communication of the exchanged data between the host computing device and the modular device so that the exchanged data must first pass through the security module; and

operably connecting the security module and/or the target module to the host computing device in response to an instruction from the host computing device.

Ex. 1001, 26:12–25, 26:34–53.

D. References Relied Upon

Petitioner relies on the following references:

Exhibit	Reference
1003	PCT Application WO 95/16238, published June 15, 1995 (“Jones”)
1004	Charles Cresson Wood & Howard M. Zeidler, <i>Security Modules: Potent Information Security System Components</i> , 5 Computers & Security 114 (1986) (“Security Modules”)
1005	<i>Common Interface Specification for Conditional Access and Other Digital Video Broadcasting Decoder Applications</i> , Digital Video Broadcasting, DVB Document A017, dated May 31, 1996 (“Common Interface Specification”)
1006	U.S. Patent No. 5,675,645, issued Oct. 7, 1997 (filed Apr. 18, 1995) (“Schwartz”)
1007	U.S. Patent No. 5,237,609, issued Aug. 17, 1993 (“Kimura”)

Pet. 3–4. Petitioner also relies on a declaration of Roy A. Griffin III, P.E. (Ex. 1010).

E. Asserted Grounds of Unpatentability

Petitioner challenges the patentability of claims 55 and 57 on the following grounds:

Reference(s)	Basis	Claim(s) Challenged
Jones	§ 102(b) or § 103(a) ²	55 and 57

² Section IV.C. at pages 4–5 of the Petition states “Jones (Ex. 1003) renders claims 55 and 57 of the ’135 patent obvious,” whereas Heading VII.A. at page 15 of the Petition identifies the same ground of challenge as

Reference(s)	Basis	Claim(s) Challenged
Jones and (Security Modules and/or Common Interface Specification)	§ 103(a)	55 and 57
Jones and (Schwartz and/or Kimura)	§ 103(a)	57

Pet. 4–5.

III. DISCUSSION

A. Claim Construction

1. Applicable Standard and General Principles

Although the '135 patent's expiration date is not mentioned by either party, we note that the '135 patent issued from an application filed June 4, 1997, and accordingly expired no later than June 4, 2017. 35 U.S.C. § 154(a)(2). Petitioner contends that, “[u]nder 37 C.F.R. § 42.100(b), a claim in *inter partes* review is given the ‘broadest reasonable construction’ in light of the specification” and that “for purposes of this *inter partes* proceeding only, that the broadest reasonable interpretation should govern the meaning of the claim terms.” Pet. 14. Petitioner disregards that section 42.100(b) states more specifically only that “[a] claim *in an unexpired patent that will not expire before a final written decision is issued* shall be given its broadest reasonable construction” (emphasis added), and that we instead construe claims of an expired patent according to the standard applied by the district courts. *See In re Rambus Inc.*, 694 F.3d 42, 46 (Fed. Cir. 2012) (“While claims are generally given their broadest possible scope during prosecution, *In re Hyatt*, 211 F.3d 1367, 1372 (Fed.

“Anticipation or Obviousness of Claims 55 and 57 Based on Jones.” We consider both anticipation and obviousness herein.

Cir. 2000), the Board’s review of the claims of an expired patent is similar to that of a district court’s review.”). Specifically, we apply the principles set forth in *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–17 (Fed. Cir. 2005) (en banc). Under that standard, the words of a claim are generally given their ordinary and customary meaning, which is the meaning the term would have to a person of ordinary skill at the time of the invention, in the context of the entire patent including the specification. See *Phillips*, 415 F.3d at 1312–13.

2. “security module” and “target module”

The terms “security module” and “target module” both are recited in each challenged claim. Petitioner identifies a dispute between itself and Patent Owner in related district court litigation as to whether those terms require only “functional (not necessarily physically distinct) modules.” Pet. 15. Specifically, Petitioner points to a statement in an infringement claim chart that appears to have been attached as an exhibit to Patent Owner’s complaint in the litigation that the accused device “has at least two modules, a security module (e.g., cryptographic functionality) and a target module (e.g., storage functionality).” *Id.* (citing Ex. 1008, 2). Petitioner states that it “expressly disagrees with Patent Owner’s broad construction of the ‘modules’ language as covering structures that are not physically distinct.” *Id.* Petitioner contends that the proper construction of “module” “requires a structure that performs as a ‘security’ module and another separate (potentially connected) structure that performs as a ‘target’ (e.g., memory module, second security module, etc.).” *Id.* at 18.

Patent Owner does not directly address Petitioner’s assertions regarding whether the recited modules must be physically or merely

functionally distinct, but instead argues Petitioner took the position in the district court litigation that the terms “security module” and “target module” invoke 35 U.S.C. § 112 ¶ 6. Prelim. Resp. 4–5 (citing Ex. 2001, 20–21). Patent Owner states that, although it disagreed with Petitioner’s position, the fact that Petitioner took those positions and yet did not identify the claimed function and specific portions of the specification that describe the corresponding structure, as required by 37 C.F.R. § 42.104(b)(3), renders the Petition deficient. *Id.* at 4 n.1, 5–6.

Despite their arguments, both parties agree that construction of “security module” and “target module” is not necessary to a determination of whether Petitioner has demonstrated a reasonable likelihood of prevailing on the asserted grounds of unpatentability. Specifically, Petitioner contends that Jones discloses the recited modules regardless of whether they must be physically or merely functionally distinct (Pet. 19), and Patent Owner contends that the Petition fails whether or not § 112 ¶ 6 is invoked by the module elements (Prelim. Resp. 4 n.1). We agree that it is unnecessary to this Decision to construe “security module” and “target module.” *See Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011) (“[C]laim terms need only be construed ‘to the extent necessary to resolve the controversy.’” (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

B. Analysis of Asserted Grounds of Unpatentability

1. General Principles

A claim is anticipated under 35 U.S.C. § 102 “only if each and every element as set forth in the claim is found, either expressly or inherently

described, in a single prior art reference.” *Verdegaal Bros., Inc. v. Union Oil Co. of Cal.*, 814 F.2d 628, 631 (Fed. Cir. 1987). Moreover,

unless a reference discloses within the four corners of the document not only all of the limitations claimed but also all of the limitations arranged or combined in the same way as recited in the claim, it cannot be said to prove prior invention of the thing claimed and, thus, cannot anticipate under 35 U.S.C. § 102.

Net MoneyIN, Inc. v. VeriSign, Inc., 545 F.3d 1359, 1371 (Fed. Cir. 2008); accord *In re Arkley*, 455 F.2d 586, 587 (CCPA 1972).

A patent claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are “such that the subject matter[,] as a whole[,] would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art³; and (4) objective evidence of nonobviousness, i.e., secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

Our Rules require that a petition for *inter partes* review identify “[h]ow the construed claim is unpatentable under the statutory grounds identified” and must specify “where each element of [a challenged] claim is

³ Petitioner proposes a definition for a person of ordinary skill in the art. Pet. 13; see Ex. 1010 ¶ 20. Patent Owner does not challenge this definition. For purposes of this Decision and to the extent necessary, we adopt Petitioner’s definition.

found in the prior art patents or printed publications relied upon.” 37 C.F.R. § 42.104(b)(4). Moreover, “a challenger who seeks to demonstrate that a means-plus-function limitation was present in the prior art must prove that the corresponding structure—or an equivalent—was present in the prior art.” *Fresenius USA, Inc. v. Baxter Int’l, Inc.*, 582 F.3d 1288, 1299 (Fed. Cir. 2009) (citing *Donaldson*, 16 F.3d 1189, 1193 (Fed. Cir. 1994) (en banc)).

2. Asserted Anticipation or Obviousness of Claims 55 and 57 over Jones

Petitioner asserts that claims 55 and 57 are unpatentable as anticipated by or obvious over Jones. Pet. 15–28. Having reviewed the Petition and Preliminary Response, as well as the presented evidence, we determine that Petitioner has not established a reasonable likelihood of prevailing on its assertion that the challenged claims are unpatentable over Jones.

a. Overview of Jones

Jones, titled “Secure Computer Memory Card,” describes a detachable memory card that may be interconnected with a host personal computer by means of a hardware and software interface in conformance with the Personal Computer Memory Card International Association (PCMCIA) standard. Ex. 1003, Title, Abstract, 4:3–7. Figures 1 and 2 of Jones are reproduced below.

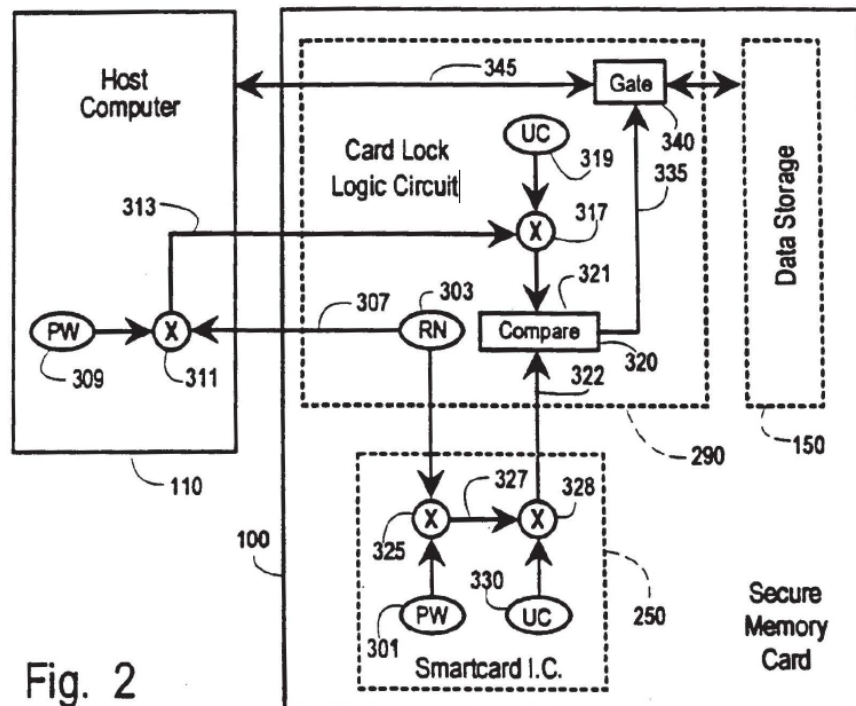
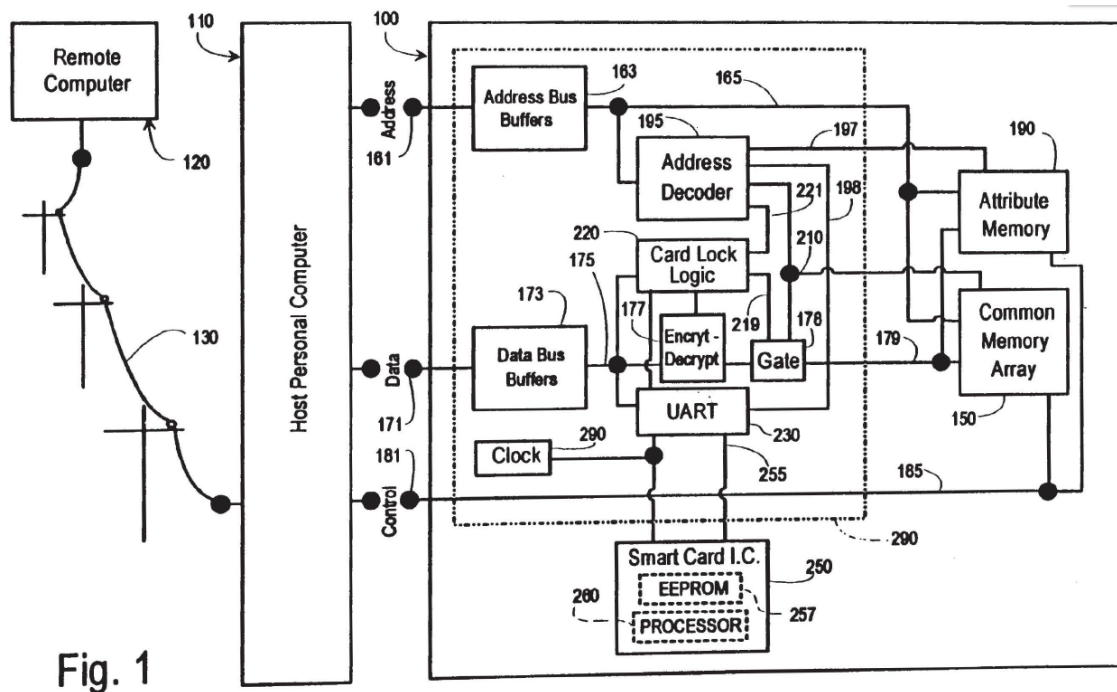


Figure 1 is a block diagram of a memory card described by Jones, shown interconnected with a host computer that is, in turn, connected to other computers by telecommunications links. Ex. 1003, 3:26–29. Figure 2

is a data flow diagram depicting a mechanism for providing password protection for information stored within a memory card of the type shown in Figure 1. *Id.* at 3:30–31. As illustrated in Figure 1, memory card 100 includes smart card integrated circuit (I.C.) 250 for storing a password, as well as logic circuitry for preventing access to information stored on the memory card unless a user of host computer 110 to which memory card 100 is connected can supply a password matching the stored password. *Id.* at Abstract. Smart card I.C. 250 may also be used to store public and private key values used to encrypt and decrypt data stored on memory card 100, elsewhere on host computer 110, or exchanged with remote computer 120. *Id.*

According to Jones, memory card 100 stores data in common memory array 150, preferably implemented with non-volatile flash memory integrated circuits. *Id.* at 4:29–30. Data transfers between common memory array 150 and host computer 110 are accomplished via interface data terminals 171, data bus buffer 173, internal data bus 175, internal encryption/decryption unit 177, gate 178, and internal data bus 179. *Id.* at 5:1–4. Control signals are exchanged between common memory array 150 and host computer 110 via PCMCIA interface control terminals 181 and internal control bus 185. *Id.* at 5:4–7.

b. Claim 55

Claim 55 recites, in part, the steps of “*receiving a request* from the host computing device for information regarding the type of the modular device” and “*providing the type of the target module to the host computing device in response to the request.*” Ex. 1001, 26:18–21 (emphasis added). In support of its contention that claim 55 is unpatentable over Jones,

Petitioner contends “Jones discloses that ‘[c]ontrol signals are exchanged between the common memory array 150 and the host computer via the PCMCIA interface control terminals 181 and an internal control bus 185,” and further quotes Jones as follows:

[T]o implement the PCMCIA interface standard, the secure memory card includes a non-volatile attribute memory 190 which stores information enabling the host computer to automatically identify the particular PCMCIA card as soon as the card and host are connected, and to automatically establish the appropriate hardware/software interface using suitable driver software which executes on the host computer 110.

Pet. 19–20 (quoting Ex. 1003, 5:24–29 (emphasis added by Petitioner)). Petitioner also argues that the Jones system “is able to identify the type of modular device even in cases wherein the host computer is not provided with PCMCIA Card Services and Socket Services functions,” pointing to disclosure in Jones that, “[f]or host computers which are not provided with standard PCMCIA Card Services and Socket Services functions, the device driver directly interrogates the CIS structures in the attribute memory” and “when the host computer is first powered up and the Client Device Driver is initialized, the Client Device Driver calls Card Services functions to process the card’s CIS entries to identify each partition that may be locked.” Pet. 20 (quoting Ex. 1003, 9:4–6, 10:14–16). Petitioner concludes, “[t]hus, a request is received from the host computing device for information regarding the type of modular device,” and “Jones discloses providing the type of the target module to the host computing device in response to the request mentioned above, as set forth above.” *Id.* at 20–21 (citing Ex. 1010 ¶¶ 49, 51).

Patent Owner responds that the PCMCIA Card Services embodiments of Jones cited by Petitioner do not indicate that the modular device responds to any request from the host computer; that the “without Card Services” embodiment is not properly combined with the PCMCIA Card Services embodiment either in an anticipation or obviousness context; and that Petitioner also fails to show that Jones discloses providing the type of target module to the host computing device “in response to the request.” Prelim. Resp. 14–17. More particularly, according to Patent Owner, although Petitioner points to Jones’s disclosure that “[c]ontrol signals are **exchanged** between the common memory array 150 and the host computers via the PCMCIA interface control terminals 181 and internal control bus 185,” “Petitioner does not explain how the **exchange** of signals teaches the **request** of information from the host to the modular device and the modular device’s response thereto.” *Id.* at 15 (citing Pet. 19; Ex. 1003, 5:4–7). Patent Owner further contends that Petitioner does not provide any explanation as to how Jones’s “automatic” identification of “*the particular PCMCIA card as soon as the card and host are connected*” relied upon by Petitioner discloses a request by the host for information from the modular device and a response thereto. *Id.* (citing Pet. 19–20; Ex. 1003, 5:24–29). As to Petitioner’s reliance on the alternative embodiment of Jones in which a host computer lacks standard Card Services and Socket Services functions, Patent Owner contends that “anticipation of a claim must be disclosed in a single embodiment in a prior art reference and, thus, this disclosure cannot provide the basis for anticipation.” *Id.* at 16 (citing Pet. 20; Ex. 1003, 9:4–6). Patent Owner additionally contends “to the extent that Petitioner meant to allege obviousness of this limitation by combining the two embodiments,

the ‘without Card Services’ embodiment teaches away from the Card Services embodiment and such a combination would not be permissible.”

Id.

We agree with Patent Owner. Petitioner does not sufficiently, persuasively explain how Jones’s disclosure of a memory card that “stores information enabling [a] host computer to automatically identify the particular . . . card as soon as the card and host are connected, and to automatically establish [an] appropriate hardware/software interface” teaches or suggests “*receiving a request* from the host computing device for information regarding the type of the modular device” and “providing the type of the target module to the host computing device *in response to the request*,” as recited in claim 55. Indeed, Jones’s statement that the card includes information enabling the host to “automatically” identify the card “as soon as the card and host are connected” suggests not only that receipt of a request is unnecessary, but also that the information is not provided “in response to [a] request.”

We also are not persuaded by Petitioner’s alternative argument based on a device driver “directly interrogat[ing] the CIS structures in the attribute memory.” Pet. 20. As Patent Owner points out (Prelim. Resp. 16), Jones describes that as separate from the embodiment relied upon by Petitioner as disclosing all other limitations of claim 55, whereas anticipation requires that all of the limitations be arranged or combined in the same way in the prior art as recited in the claim. *Net MoneyIN*, 545 F.3d at 1371. Moreover, because Petitioner does not advance any argument that the “CIS structures in the attribute memory” perform the remaining claim steps or explain how the “operably connecting” step of claim 55 would be taught or suggested by

Jones “in cases wherein the host computer is not provided with PCMCIA Card Services and Socket Services functions,” we agree with Patent Owner that this alternative argument also fails to establish a reasonable likelihood that Petitioner would prevail in its obviousness challenge to claim 55 over Jones.

c. Claim 57

Claim 57 recites, in part, the steps of “*communicating with the host computing device to exchange data between the host computing device and the modular device*” and “*performing one or more security operations and the defined interaction on the exchanged data.*” Ex. 1001, 26:42–46.

Petitioner contends with respect to the first of these steps that “[t]he preferred embodiments [of the ’135 patent] utilize a PCMCIA bus to communicate with the host computing device to exchange data.” Pet. 24 (citing Ex. 1001, Fig. 1; Ex. 1010 ¶ 59). In support of its contention that Jones teaches or suggests this step, Petitioner merely asserts that “Jones discloses using the same bus (i.e., PCMCIA) for communication between the host and the modular device.” *Id.* (citing Ex. 1003, 4:1–15; Ex. 1010 ¶ 60). With respect to the step of “performing one or more security operations and the defined interaction on the exchanged data,” Petitioner contends that “Jones’s modular device performs one or more security operations on the exchanged data,” including “selectively enabl[ing] and disabl[ing] the exchange of data between a host and modular device based upon a security comparison involving a password,” and “[i]f the comparison involving the password is successful, the defined interaction (i.e., the transfer of data between the host computer 110 and the data storage 150) is effected.” *Id.* at

24–26 (citing Ex. 1003, 7:16–8:12, 11:15–20, Figs. 1, 2; Ex. 1010 ¶¶ 62–64).

Patent Owner responds that Petitioner’s contention that communicating data, without more, satisfies both the “communicating with the host computing device” and “performing one or more security operations and the defined interaction on the exchange[d] data” limitations of claim 57 “renders [the] ‘defined interaction on the exchanged data’ limitation meaningless.” Prelim. Resp. 19. Patent Owner contends that “[b]ecause Petitioner has not offered a construction for ‘defined interaction on the exchanged data,’ and because Petitioner has not differentiated this term from the communicated limitation, this Ground is deficient.” *Id.*

We again agree with Patent Owner. Petitioner does not identify, in connection with the “communicating” step of claim 57, any disclosure in Jones of “communicating . . . to exchange data between [a] host computing device and [a] modular device.” See Pet. 24. Rather, the only disclosure Petitioner identifies in Jones of any such communication is the transfer of data between host computer 110 and data storage 150 that Petitioner relies upon as corresponding to the step of “performing . . . the defined interaction on the exchanged data.” Pet. 26 (citing Ex. 1003, 11:15–20). As Patent Owner points out, however, “[t]he claims explicitly require ‘communicating . . . to exchange data’ as a separate limitation from ‘performing one or more security operations and the defined interaction on the exchanged data’” (Prelim. Resp. 20), and thus, the “defined interaction on the exchanged data” cannot simply be the transfer of data that satisfies the “communicating . . . to exchange data” step. In other words, because Petitioner does not identify any disclosure in Jones of “communicating . . . to exchange data” as a step

separate from the exchange alleged to teach the “perform[ance of] . . . the defined interaction,” Petitioner has not established a reasonable likelihood of prevailing in showing that Jones anticipates or renders obvious the subject matter of claim 57.

3. *Remaining Grounds*

Petitioner asserts that claims 55 and 57 also are unpatentable over the combination of Jones and Security Modules and/or Common Interface Specification and that claim 57 is unpatentable over the combination of Jones and Schwartz and/or Kimura. Pet. 28–33. Petitioner does not rely in the Petition on Security Modules or Common Interface Specification to teach or suggest “*receiving a request* from the host computing device for information regarding the type of the modular device” and “providing the type of the target module to the host computing device *in response to the request*,” as recited in claim 55. Petitioner also does not rely in the Petition on Security Modules, Common Interface Specification, Schwartz, or Kimura to teach or suggest “communicating with the host computing device” and “performing one or more security operations and the defined interaction on the exchange[d] data,” as recited in claim 57, but instead relies solely on Jones for those limitations. Accordingly, for the same reasons as set forth in § III.B.2 with respect to the alleged grounds based on Jones alone, we conclude that Petitioner has not established a reasonable likelihood that it would prevail in showing that claims 55 and 57 are unpatentable on either of the remaining proffered grounds, and we do not institute an *inter partes* review on those grounds.

C. Conclusion

For the reasons discussed above, Petitioner has not established a reasonable likelihood that it would prevail with respect to any of the claims challenged in the Petition.

IV. ORDER

Accordingly, it is

ORDERED that the Petition is *denied*, and no *inter partes* review is instituted on any asserted ground.

IPR2017-00825
Patent 6,003,135

PETITIONER:

David Hoffman
FISH & RICHARDSON P.C.
hoffman@fr.com

Martha Hopkins
LAW OFFICES OF S.J. CHRISTINE YANG
mhopkins@sjclawpc.com

PATENT OWNER:

Vincent J. Rubino, III
Peter Lambrianakos
BROWN RUDNICK LLP
vrubino@brownrudnick.com
plambrianakos@brownrudnick.com