UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ASKELADDEN L.L.C.,
Petitioner,

v.

DIGITAL VERIFICATION SYSTEMS LLC,
Patent Owner.

Case IPR2018-00746
Patent 9,054,860 B1

Before JAMESON LEE, DANIEL J. GALLIGAN, and AMBER L. HAGY, *Administrative Patent Judges.*

LEE, *Administrative Patent Judge*.

DECISION
Institution of *Inter Partes* Review
35 U.S.C. § 314(a)

I. INTRODUCTION

A. Background

On March 6, 2018, Petitioner[1] filed a Petition (Paper 1, "Pet.") to institute *inter partes* review of claims 23–39 of U.S. Patent No. 9,054,860 B1 (Ex. 1001, "the '860 patent"). Patent Owner[2] did not file a Preliminary Response.

To institute an *inter partes* review, we must determine that the information presented in the Petition and any preliminary response show "that 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). Having considered the Petition and its supporting evidence, we determine that Petitioner has shown a reasonable likelihood that it would prevail in establishing the unpatentability of each of claims 26, 27, 30–34, 37, and 38.

We institute an *inter partes* review of all challenged claims 23–39 of the '860 patent with respect to all grounds of unpatentability presented in the Petition. *See SAS Inst., Inc*. v. *Iancu*, 138 S. Ct. 1348, 1359–60 (2018).

B. Related Matters

Petitioner identifies multiple district court actions in the Eastern District of Texas and the Northern District of California as related matters. Pet. 3. Patent Owner, on the other hand, has not identified any. Paper 5, 1. Petitioner also has filed a separate petition for *inter partes* review of claims 1–22 of the '860 patent, in Case IPR12018-00745. Pet. 4.

[1] Askeladden L.L.C.

[2] Digital Verification Systems, LLC.

C. The ’860 Patent (Ex. 1001)

The ’860 patent is directed to a digital verified identification system and method. Ex. 1001, 1:65–66. According to the ’860 patent, there was a need in the art for a digital verified identification system “structured to facilitate authenticating and/or verifying the identity of an electronic signatory to a file and/or otherwise structured to associate an electronic file with one or more entities.” *Id.* at 1:37–41. A “module generating assembly” is provided, which creates at least one digital identification module to be embedded or otherwise disposed within one or more electronic files. *Id.* at 1:66–2:3. The digital identification modules are structured to be associated with one or more entities such as an individual, a group of individuals, and/or a signatory of a document or file. *Id.* at 3:25–30. Such modules may include “virtually any file, item, object, or device” structured to be embedded or otherwise disposed within an electronic file or document. *Id.* at 3:31–35. For example, the digital identification module can include an image or photographic file. *Id.* at 3:35–37.

An entity, such as the signatory of an electronic document, may communicate at least one verification data element to the module generating assembly prior to creation of the digital identification module. *Id.* at 2:3–6. The verification data element or elements may include any indicia or data that facilitate the verification or identification of the corresponding entity, such as username, password, date of birth, social security number, driver’s license number, or credit card number. *Id.* at 2:6–12. In one embodiment, the digital identification module includes a file or object that may be imported into a computer application to facilitate embedding or otherwise disposing the digital identification module into an electronic file such as a word processing document. *Id.* at 2:13–18. Also, in one embodiment, the module generating assembly is at least partially integrated within the computer application, e.g., an interactive word processing program, such that the digital identification module created therefrom may be directly embedded within the electronic file rather than first imported into the computer application. *Id.* at 2:19–24.

The digital identification module of at least one embodiment includes at least one primary component and at least one metadata component. *Id.* at 2:25–27. The primary component may include a digital representation of a signature and/or one or more reference codes, numbers, or characters, and is generally visible or perceptible to a reader, recipient, or other user of the electronic document. *Id.* at 2:27–33. A reader, recipient, or other user of the electronic file may access some or all of the metadata components of the digital identification module by hovering a mouse or other pointing device over the visible portion of the digital identification module and clicking on it. *Id.* at 2:38–43.

D. Illustrative Claims

Of the challenged claims, claims 23, 26, and 39 are the only independent claims and are reproduced below:

> 23. A digital verified identification system, comprising:
>
> a module generating assembly structured to receive at least one verification data element corresponding to at least one entity and create at least one digital identification module, wherein said at least one digital identification module is structured to be associated with said at least one entity;
>
> said at least one digital identification module further structured to be embedded within at least one electronic file,

said at least one digital identification module comprising at least one primary component structured to at least partially associate said at least one digital identification module with said at least one entity, wherein said at least one primary component includes a digital signature, wherein

said at least one digital identification module is cooperatively structured to be embedded within only a single electronic file.

26. A method of digital identification verification, comprising:

receiving at least one verification data element from an entity,

creating at least one digital identification module corresponding to the entity, wherein the digital identification module includes at least one primary component at least partially associated with the entity, and

embedding the at least one digital identification module within an electronic file, wherein

said at least one digital identification module is cooperatively structured to be embedded within only a single electronic file.

39. A method of verifying the identification of an entity associated with an electronic file, comprising:

receiving at least one verification data element from the entity,

creating at least one digital identification module corresponding to the entity by at least partially combining a primary component with at least one metadata component, wherein the primary component includes a digital signature, and

embedding the at least one digital identification module within the electronic file, wherein

said at least one digital identification module is cooperatively structured to be embedded within only a single electronic file.

Ex. 1001, 10:36–53, 10:60–11:5, 12:14–27.

E. Evidence Relied Upon by Petitioner

Petitioner relies on the following references:

Reference		Date	Exhibit
Houser	U.S. Patent No. 5,606,609	Feb. 25, 1997	1005
Mansz	U.S. Pub. App. 2006/0259767 A1	Nov. 16, 2006	1007
Gupta	U.S. Patent No. 8,205,087 B2	June 19, 2012	1011

Petitioner also relies on the Declarations of Mr. Ivan Zatkovich (Ex. 1002) and Mr. Roderick R. McKelvie (Ex. 1012).[3]

F. The Asserted Grounds of Unpatentability

Petitioner asserts the following grounds of unpatentability (Pet. 6):

Claim(s) Challenged	Basis	Reference(s)
23–31, 33–36, and 39	§ 102(b)	Houser
32 and 37	§ 103(a)	Houser and Mansz
38	§ 103(a)	Houser, Mansz, and Gupta

II. ANALYSIS

A. Claim Construction

In an *inter partes* review, claim terms in an unexpired patent are interpreted according to their broadest reasonable construction in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b); *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2142–46 (2016). Consistent with that standard, claim terms are generally given their ordinary

[3] The testimony of Mr. McKelvie pertains not to the merits of the alleged anticipation or obviousness but to who constitutes a real party in interest.

and customary meaning, as would have been understood by one of ordinary skill in the art in the context of the entire disclosure. *See In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). There are, however, two exceptions to that rule: "1) when a patentee sets out a definition and acts as his own lexicographer," and "2) when the patentee disavows the full scope of a claim term either in the specification or during prosecution." *Thorner v. Sony Comput. Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012). Disavowal can be effectuated by language in the specification or the prosecution history. *Poly-America, L.P. v. API Indus., Inc.*, 839 F.3d 1131, 1136 (Fed. Cir. 2016). "In either case, the standard for disavowal is exacting, requiring clear and unequivocal evidence that the claimed invention includes or does not include a particular feature." *Id.*

Only terms that are in controversy need to be construed, and only to the extent necessary to resolve the controversy. *See Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011); *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999).

"module generating assembly structured to receive at least one verification data element corresponding to at least one entity and create at least one digital identification module"

Under 35 U.S.C. § 112, paragraph 6, "[a]n element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof."[4]

Claim 23 recites a "module generating assembly structured to receive at least one verification data element corresponding to at least one entity and create at least one digital identification module." Ex. 1001, 10:37–40. This phrase, containing a functional limitation, does not include the word "means" and thus presumptively is not a means-plus-function limitation under 35 U.S.C. § 112, paragraph 6. *Williamson*, 792 F.3d at 1348. However, that presumption can be overcome when the phrase does not recite sufficiently definite structure or recites function without sufficient structure for performing that function. *Id.* at 1349. That is the case here.

The term "assembly" is so broad that it does not sufficiently convey definite structure. As the Federal Circuit has stated, "[g]eneric terms such as 'mechanism,' 'element,' 'device,' and other nonce words that reflect nothing more than verbal constructs may be used in a claim in a manner that is tantamount to using the word 'means' because they 'typically do not connote sufficiently definite structure.'" *Id.* at 1350 (citation omitted). In this case, "assembly" is used as a generic place-holder for anything that performs the recited function, much as the word "means" does. The words before and after "assembly" are "module generating" and "structured to receive at least one verification data element corresponding to the at least one entity and create said at least one digital identification module." Those recitations are

[4] Paragraphs 1–6 of § 112 were replaced with §§ 112(a)–(f) when § 4(c) of the Leahy-Smith America Invents Act, Pub. L. No. 112–29, 125 Stat. 284, 329 (2011) ("AIA") took effect on September 16, 2012. Because the patent application resulting in the '860 patent was filed before the effective date of the AIA, we refer to the pre-AIA version of 35 U.S.C. § 112.

not structural but functional. The words "structured to" are generic and do not impart specific structure. Rather, they literally would cover any structure that performs the function that follows. Furthermore, the entire phrase reflects the typical format of a means-plus-function element that does employ the word "means," with "assembly" substituting for "means" and "structured to" used in place of "for."

Accordingly, the non-means presumption is overcome by the absence of sufficiently definite structure in the language used and by the fact that the language at issue recites function without sufficient structure for performing that function. We construe the phrase "a module generating assembly structured to receive at least one verification data element corresponding to at least one entity and create at least one digital identification module" as a means-plus-function element under 35 U.S.C. § 112, paragraph 6. The function recited is "receive at least one verification data element corresponding to at least one entity and create at least one digital identification module." The words "module generating" preceding "assembly" are simply part of the name for the element and do not change the function recitation after "assembly."

For a means-plus-function limitation, Petitioner is required to "identify the specific portions of the specification that describe the structure, material, or acts corresponding to each claimed function." 37 C.F.R. § 42.104(b)(3). As the Federal Circuit has noted: "structure disclosed in the specification is 'corresponding' structure *only* if the specification or prosecution history clearly links or associates that structure to the function recited in the claim. This duty to link or associate structure to function is the *quid pro quo* for the convenience of employing § 112, ¶ 6." *Saffran v.*

Johnson & Johnson, 712 F.3d 549, 562 (Fed. Cir. 2013) (quoting *B. Braun Med., Inc. v. Abbott Labs.*, 124 F.3d 1419, 1424 (Fed. Cir. 1997)); *see also Noah Sys, Inc. v. Intuit Inc.*, 675 F.3d 1302, 1312 (Fed. Cir. 2012).

With respect to the means-plus-function limitation of a "module generating assembly structured to receive at least one verification data element corresponding to at least one entity and create at least one digital identification module," Petitioner has not identified sufficient corresponding structure described in the Specification of the '860 patent for performing the recited receiving and the recited creating. The closest Petitioner comes to making that identification is this: "An entity 30 (e.g., a signatory to a document, Ex1001, 3:25–30) provides a 'data verification element' 52 (e.g., username, password, SSN, driver's license number) corresponding to the entity to 'module generating assembly' 50 (e.g., a computer program). (*Id.*, 3:25–30, 3:55–67, 4:5–13)." Pet. 6–7. Thus, at best, even assuming that Petitioner even intended to identify corresponding structure, Petitioner has identified the corresponding structure only generally as "a computer program."

The reference to "a computer program" is too generic to identify any specific structure. In *Aristocrat Technologies Australia Pty Ltd. v. International Game Technology*, 521 F.3d 1328, 1333 (Fed. Cir. 2008) (quoting *Harris Corp. v. Ericsson Inc.*, 417 F.3d 1241, 1249 (Fed. Cir. 2005)), the Federal Circuit stated that "the corresponding structure for a § 112 ¶ 6 claim for a computer-implemented function is *the algorithm disclosed in the specification*." *Id.* (emphasis added). As the Federal Circuit explained, "a general purpose computer programmed to carry out a particular algorithm creates a 'new machine' because a general purpose computer 'in effect becomes a special purpose computer once it is programmed to perform particular functions pursuant to instructions from program software.'" *Id.*; *see also WMS Gaming, Inc. v. Int'l Game Techs.*, 184 F.3d 1339, 1349 (Fed. Cir. 1999). Consequently, the specification must disclose enough of a specific algorithm to provide the necessary structure under § 112, sixth paragraph. *Finisar Corp. v. DirectTV Grp., Inc.*, 523 F.3d 1323, 1340 (Fed. Cir. 2008). Allowing a computer programmed to perform a specialized function to be claimed without disclosure of the algorithm used for that programming would exhibit the same type of impermissible overbreadth of purely functional claims. *Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1367 (Fed. Cir. 2008).

> If special programming is required for a general-purpose computer to perform the corresponding claimed function, then the default rule requiring disclosure of an algorithm applies. It is only in the rare circumstances where any general-purpose computer without any special programming can perform the function that an algorithm need not be disclosed.

Ergo Licensing, LLC v. CareFusion 303, Inc., 673 F.3d 1361, 1365 (Fed. Cir. 2012); *see also Williamson*, 792 F.3d at 1352 ("In cases . . . involving a claim limitation that is subject to § 112, para. 6 that must be implemented in a special purpose computer, this court has consistently required that the structure disclosed in the specification be more than simply a general purpose computer or microprocessor. . . . [T]he specification [must] disclose an algorithm for performing the claimed function." (citations omitted)).

By simply noting that the module generating assembly can be a computer program, Petitioner has not identified the underlying algorithm of any such program. This is not a circumstance falling within the narrow exception explained in *In re Katz Interactive Call Processing Patent*

Litigation, 639 F.3d 1303, 1316 (Fed. Cir. 2011), where the function recited is generic and can be performed by any general-purpose computer without special programming, *e.g.*, "processing," "receiving," "storing." The specialized function here includes "creat[ing] said at least one digital identification module," where the digital identification module is limited by other claim language as "cooperatively structured to be embedded within only a single electronic file." Petitioner makes no explanation as to why the recited function would be so basic that it could be performed by a general purpose computer without any special programming. Accordingly, Petitioner has not identified corresponding structure, described in the Specification of the '860 patent, that causes a computer to perform the recited function of "receive at least one verification data element corresponding to at least one entity and create at least one digital identification module."

"said at least one digital identification module is cooperatively structured to be embedded within only a single electronic file"

Each of independent claims 23, 26, and 39 recites: "said at least one digital identification module is cooperatively structured to be embedded within only a single electronic file." The words "cooperatively structured" do not appear in the Specification of the '860 patent as filed, except in initially filed application claims 17 and 26, each of which recites: "wherein said at least one digital identification module is cooperatively structured to be embedded within a single electronic file." Ex. 1004, 23, 25. It is not clear, based on the Specification as filed, what "cooperatively structured" means. During examination, Applicants by amendment added such a limitation into independent application claims 1, 24, 31, and 44 to distinguish prior art applied by the Examiner, and they explained what "cooperatively structured" means in the context of that limitation:

> Moreover, the limitations at issue describe that the digital identification module is "cooperatively structured," yet the Examiner's analysis gives no patentable weight to the limitation of "cooperatively." Properly construed, the digital identification module is matched with the single electronic file (i.e., cooperatively) such [that] the digital identification module is usable only with the single electronic file. These limitations, however, have not been addressed by the Examiner's analysis.

Ex. 1004, 167:22–168:3, 168:23–28.[5] Ultimately, application claims 1, 24, 31, and 44 issued as patent claims 1, 23, 26, and 39, respectively. *Id.* at 368–69.

Based on the prosecution history as noted above, the limitation "said at least one digital identification module is cooperatively structured to be embedded within only a single electronic file" means the digital identification module is matched specifically with something about an electronic file, such that the digital identification module is usable only with that single electronic file.

B. Alleged Anticipation of Claims 23–31, 33–36, and 39 by Houser

1. The Law on Anticipation

To establish anticipation, each and every element in a claim, arranged as recited in the claim, must be found in a single prior art reference.

[5] Subsequent to the amendment, the Examiner maintained the prior art rejection, and Applicants appealed to the Patent Trial and Appeal Board. Pet. 15; Ex. 1004, 238. On appeal, the rejection was reversed, with the Board stating that the Examiner had not persuasively explained how the "within only a single electronic file" limitation was met. Ex. 1004, 357.

Net MoneyIN, Inc. v. VeriSign, Inc., 545 F.3d 1359, 1369 (Fed. Cir. 2008); *Karsten Mfg. Corp. v. Cleveland Golf Co.*, 242 F.3d 1376, 1383 (Fed. Cir. 2001). Although the elements must be arranged in the same way as is recited in the claim, "the reference need not satisfy an *ipsissimis verbis* test." *In re Gleave*, 560 F.3d 1331, 1334 (Fed. Cir. 2009); *In re Bond*, 910 F.2d 831, 832–33 (Fed. Cir. 1990)). Thus, identity of terminology between the prior art reference and the claim is not required. "A reference anticipates a claim if it discloses the claimed invention 'such that a skilled artisan could take its teachings in *combination with his own knowledge of the particular art and be in possession of the invention.*'" *In re Graves*, 69 F.3d 1147, 1152 (Fed. Cir. 1995) (quoting *In re LeGrice*, 301 F.2d 929 (CCPA 1962)). Prior art references must be "considered together with the knowledge of one of ordinary skill in the pertinent art." *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994) (citation omitted).

Also, "it is proper to take into account not only specific teachings of the reference but also the inferences which one skilled in the art would reasonably be expected to draw therefrom." *In re Preda*, 401 F.2d 825, 826 (CCPA 1968). As the Court of Appeals for the Federal Circuit recently explained, the dispositive question for anticipation is whether one skilled in the art would reasonably understand or infer from a prior art reference that every claim element is disclosed in that reference. *Eli Lilly v. Los Angeles Biomedical Research Inst.*, 849 F.3d 1073, 1074–1075 (Fed. Cir. 2017).

2. Level of Ordinary Skill in the Art

Petitioner proposes that the level of ordinary skill in the art is reflected by the prior art of record. Pet. 18. Alternatively, Petitioner proposes that the level of ordinary skill is at the education level of a bachelor's degree in computer science "or a related study" and at the experience level of "two years of experience with data and file security and user authentication methods or the equivalent." *Id.* We find the phrase "or a related study" to be excessively vague. Instead, we agree with Petitioner's first proposal, i.e., in this case, the level of ordinary skill in the art is reflected by the prior art of record. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001); *In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995); *In re Oelrich*, 579 F.2d 86, 91 (CCPA 1978).

3. Claims 23–25

Claim 23 is independent and each of claims 24 and 25 depends from claim 23. One of the elements recited in claim 23 is a "module generating assembly structured to receive at least one verification data element corresponding to at least one entity and create at least one digital identification module." As discussed above, this is a means-plus-function element under 35 U.S.C. § 112, sixth paragraph.

For this element, because Petitioner does not "identify the specific portions of the specification that describe the structure, material, or acts corresponding to each claimed function," as required by our Rules (37 C.F.R. § 42.104(b)), to enable us to determine if the asserted prior art teaches such structure, Petitioner's contentions are inadequate for the alleged anticipation of claims 23, 24, and 25 by Houser.

4. Houser

Houser relates to "a system and method for verifying and indicating the integrity, source, and/or approval status of an electronic document, and more particularly to a method and apparatus for embedding a security object including security information into an electronic document and for using the embedded security object to invoke verification processing of the security information and the electronic document to verify the integrity, source, and/or approval status of the electronic document." Ex. 1005, 1:7–18.

The system and method of Houser include a security information assembler that assembles security information into a predetermined format and a security object embedder that embeds a security object that includes the security information and an identifier that would invoke processing of the security information into an electronic document. *Id.* 3:50–59. The system and method of Houser further include an embedded security information extractor that extracts security information from the embedded security object. *Id.* at 3:61–65. Also provided is a verification processor that processes the extracted information to verify at least one aspect of the signed electronic document. *Id.* at 3:65–67. The verification processor thus verifies the "signature" in the electronic document. *Id.* at 3:67–4:2.

"[T]he security information may include a document digest and/or a signature digest." *Id.* at 4:11–12. "The document digest includes one or more data items that characterize the electronic document at the time the security object is embedded, such as a hash value," and "[t]he signature digest includes one or more data items that characterize the signator or the instance of the embedded security object, such as a serial number that is unique for each embedded security object." *Id.* at 4:11–18, 5:31–33. The verification processor may include a calculator for calculating a data item that characterizes the current content of an electronic document and a comparator for comparing the data item in the extracted security information with the calculated data item. *Id.* at 5:36–40. A verification detector may then detect that the electronic document was modified if the extracted data item does not match the calculated data item or that the electronic document was not modified if the extracted data item matches the calculated data item. *Id.* at 5:40–46. For example, the extracted data item may be an embedded hash value associated with the original document and the calculated data item may be a calculated hash value of the current document. *Id.* at 5:46–48.

Additionally, an electronic chop may be provided in the security information, and, if so, the system may include a display controller for controlling a display device to display the electronic chop in the signed document only if the verification processor verifies the signed electronic document. *Id.* at 4:46–51.

5. Independent Claims 26 and 39

Claim 26 recites "[a] method of digital identification verification." Ex. 1001, 10:60. Petitioner points to the Abstract of Houser, which states:

> The integrity or the signator of an electronic document can be verified by embedding a security object . . . . The signator of the electronic document can be verified based upon the result of the decryption. The integrity of the electronic document can be verified if the decrypted document digest matches the calculated document digest.

Ex. 1005, Abstr., *cited in* Pet. 37. Petitioner further cites to other portions of Houser. Pet. 37–38 (citing Ex. 1005, 7:29–31, 8:43–49). We are sufficiently persuaded that Houser discloses "a method of digital identification verification."

Claim 26 recites a step of: "receiving at least one verification data element from an entity." Ex. 1001, 10:62–63. Petitioner identifies portions of Houser that describe receiving a password, for preventing unauthorized access, or system identification data from a user. Pet. 38 (citing Ex. 1005, 9:21–36, 11:2–4, 11:26–29, Figs. 3C, 7A–7E). Petitioner regards, within

Houser, the user's password and system identification data as data verification elements. *Id.* Based on the evidence cited by Petitioner, we are sufficiently persuaded that both the user's password and user's system identification information constitute a data verification element, and that Houser discloses "receiving at least one verification data element from an entity." Specifically, the user is that entity.

Claim 26 recites a step of "creating at least one digital identification module corresponding to the entity, wherein the digital identification module includes at least one primary component at least partially associated with the entity." Ex. 1001, 10:64–67. Petitioner identifies Houser's "security object" as the claimed digital identification module corresponding to the entity, and cites the following text from Houser:

> The embedded security object includes security information and an identifier for invoking verification processing of the security information to verify at least one aspect or characteristic of the electronic document, for example, document integrity and/or the identity of one or more "signators" who embedded security objects in the electronic document.

Pet. 39 (quoting Ex. 1005, 7:31–37). Petitioner identifies Houser's "electronic chop," or a signature graphic that implements Houser's electronic chop, as the primary component of the digital identification module that is at least partially associated with the entity. Pet. 39–41. Houser, as cited by Petitioner (Pet. 39), describes that the security information may include an electronic chop (Ex. 1005, 7:53–54) and that the electronic chop may be an arbitrary static graphic object for use as the user's personal electronic indicia (Ex. 1005, 10:23–27). The testimony of Mr. Zatkovich confirms the same. Ex. 1002 ¶¶ 77–78. Based on the evidence cited by Petitioner, we are sufficiently persuaded that Houser discloses the step of: "creating at least one digital identification module corresponding to the entity, wherein the digital identification module includes at least one primary component at least partially associated with the entity."

Claim 26 recites a step of "embedding the at least one digital identification module with an electronic file." Ex. 1001, 11:1–2. Petitioner cites to the following portions of Houser as disclosing embedding the at least one digital identification module (Houser's security object) within an electronic file (Pet. 42):

> After the document is created, an electronic document security application 120 may be used to embed a security object in the electronic document as represented at 130. The embedded security object includes security information and an identifier for invoking verification processing of the security information to verify at least one aspect or characteristic of the electronic document, for example, document integrity and/or the identity of one or more "signators" who embedded security objects in the electronic document.

Ex. 1005, 7:29–37.

> The general function of the signature insertion module 240 is to assemble the security information and to embed the assembled security information as a security object, for example, in the electronic document.

Id. at 13:24–28.

> To insert an electronic chop in the document, the user first positions the cursor at a point in the electronic document where the electronic chop is to be inserted. . . . After setting available parameters, the user may enter an instruction, for example, by selecting an "OK" button, that causes a security object, including the selected electronic chop, to be embedded in the electronic document.

Id. at 13:36–60. The testimony of Mr. Zatkovich confirms the same. Ex. 1002 ¶¶ 84–86. Based on the evidence cited by Petitioner, we are sufficiently persuaded that Houser discloses the step of: "embedding the at least one digital identification module with an electronic file."

Claim 26 recites: "said at least one digital identification module is cooperatively structured to be embedded within only a single electronic file." Ex. 1001, 11:3–5. We have construed above the phrase "said at least one digital identification module is cooperatively structured to be embedded within only a single electronic file" to mean that the digital identification module is matched specifically with something about an electronic file, such that the digital identification module is usable only with that single electronic file.

Petitioner explains that because Houser's embedded security object includes one or more data items that characterize the particular electronic document at the time the security object is embedded into the document, such as a hash value of the entire document, it "is cooperatively structured to be embedded within only a single electronic file." Pet. 43 (citing Ex. 1005, 12:40–54, 13:4–20, 14:10–24, 16:10–23, 16:34–51). Petitioner further notes that Houser describes that any change in a document after embedding of the security object may cause the digital signature to be removed or not displayed or printed, and Petitioner indicates that such disclosure further confirms that the security object is cooperatively structured with respect to the file in which it is embedded. Pet. 43. The testimony of Mr. Zatkovich supports Petitioner's assertions. Ex. 1002 ¶ 89. Based on the evidence presented by Petitioner, we are sufficiently persuaded that Houser discloses the limitation of: "wherein said at least one digital identification module is cooperatively structured to be embedded within only a single electronic file."

Independent claim 39 is essentially the same as independent claim 26, except that (1) the preambles of the two claims are different, (2) claim 39 recites combining the primary component with at least one metadata component, and (3) claim 39 recites that the primary component includes a digital signature. With regard to the preambles, claim 26 recites "[a] method of digital identification verification," and claim 39 recites "[a] method of verifying the identification of an entity associated with an electronic file." The above discussion in the context of claim 26 with regard to verification processing to verify the identity of a signator to the document accounts for the preamble recitation of claim 39. Specifically, Houser describes:

> The embedded security object includes security information and an identifier for invoking verification processing of the security information to verify at least one aspect or characteristic of the electronic document, for example, document integrity and/or the identity of one or more "signators" who embedded security objects in the electronic document.

Ex. 1005, 7:31–37. Additionally, Houser further describes the following:

> An electronic chop also may be provided in the security information. If so, the electronic document verification system may include a display controller for controlling a display device to display the electronic chop in the signed electronic document only if the verification process verifies the signed electronic document.

Id. 4:47–52. Accordingly, we are sufficiently persuaded that the preamble of claim 39 is met by Houser. Alternatively, we find that the preamble of claim 39 does not recite an essential step in light of the recitations in the body of the claim and because it is not necessary to give life, meaning, and vitality to the claim. *See Pitney Bowes, Inc. v. Hewwlett-Packard Co.*, 182 F.3d 1298, 1305 (Fed. Cir. 1999). For instance, the body of claim 39 does not depend on the preamble for completeness. *Cf. Catalina Marketing Int'l., Inc. v. Coolsavinmgs.com, Inc.*, 289 F.3d 801, 808 (Fed. Cir. 2002).

As discussed above in the context of claim 26, Petitioner has identified Houser's electronic chop or signature graphic as the primary component of the digital verification module (Houser's security object). Pet. 40–41. Here, Petitioner identifies Houser's electronic chop or signature graphic as that which satisfies claim 39's requirement of the primary component including a digital signature. Pet. 55. On the evidence before us, we find that Houser's electronic chop or signature graphic, the primary component, itself constitutes a digital signature and therefore includes a digital signature.

Finally, however, Petitioner's discussion of claim 39 does not address how Houser meets the recitation in claim 39 of partially combining the primary component with at least one metadata component. *Id.* at 54–55. In that context, Petitioner has not even identified any metadata component that is partially combined with Houser's electronic chop or signature graphic.

For the foregoing reasons, Petitioner has shown a reasonable likelihood that it would prevail in establishing that claim 26 is anticipated by Houser.

6. Dependent Claims 27, 30, 31, 33, and 34

Claim 27 depends from claim 26 and further recites: "further comprising defining receiving at least one verification data element from the entity as receiving a valid username and password from the entity." Petitioner adequately accounts for this added limitation by citing the following text from Houser:

> For example, the installer module 210 may prompt the user to enter his name and an access password, respectively. The name and access password may be entered using an input device such as a keyboard, mouse, tracking ball, or other conventional input device. The access password serves to prevent unauthorized access to the various features of the electronic document security application, such as the signature insertion module 240.

Ex. 1005, 9:23–34, *quoted in* Pet. 45. The testimony of Mr. Zatkovich confirms the same. Ex. 1002 ¶ 81. Based on the evidence presented by Petitioner, we are sufficiently persuaded that Houser discloses the limitation of "further comprising defining receiving at least one verification data element from the entity as receiving a valid username and password from the entity."

Claim 30 depends from claim 26 and recites: "further comprising combining at least one primary component with at least one metadata component to at least partially create the at least one digital identification module." Petitioner regards Houser's "signature digest" as the metadata component. Pet. 47. Petitioner adequately accounts for the added limitation of claim 30 by citing the following disclosures of Houser:

> The security object may include, in addition or in the alternative, a signature digest including one or more data items which identify the signator and/or characterize or relate to the instance of the embedded security object. For example, the signature digest may include the signator's name, other information specific to the signator such as local access network (LAN) user name, LAN subdirectory specification or an Internet address, system identification, the date and time [sic] the security object is embedded, a serial number assigned to the instance of the embedded security object, information identifying the version of the electronic document security application, the signator's comments, information relating to the generation of time-varying data, other information relating to the security

> object embedding event, or any combination thereof. In addition, the security object may include the electronic chop.
>
> In one preferred embodiment, the security information includes a document digest, a signature digest, and the electronic chop. In particular, the document digest may include a hash value of the electronic document, electronic document name and path, number of pages, number of characters per page, and the date and time the document was saved. The signature digest may include user name, system identification, serial number, the version of the electronic document security application that created the security information, user comments, and date and time that the security object was embedded.

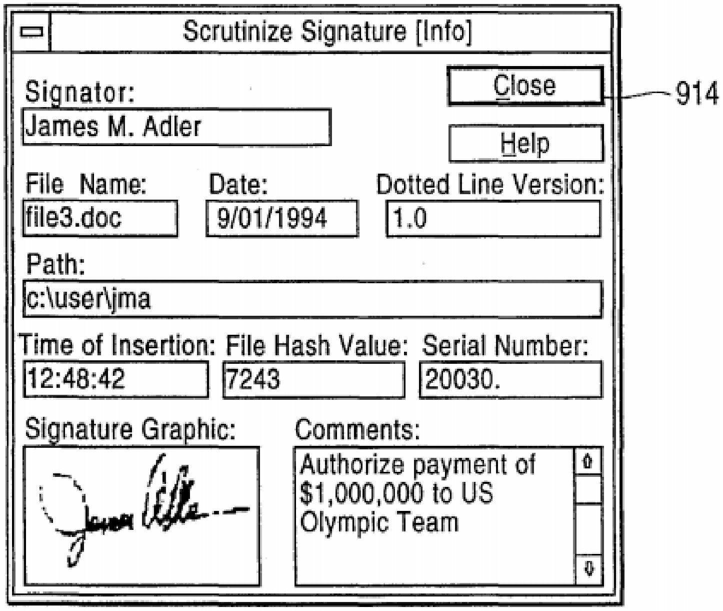
Ex. 1005, 12:55–13:14, *quoted in* Pet. 47–48. Houser also describes that "[u]pon entry of the command to embed a security object, the security information assembler 610 assembles the security information [document digest, signature digest, and electronic chop] for embedding in the document in a predetermined format." *Id.* at 14:11–14. We are sufficiently persuaded that Houser discloses the limitation of "further comprising combining at least one primary component with at least one metadata component to at least partially create the at least one digital identification module."

Claim 31 depends from claim 30 and recites "further comprising activating the digital identification module in response to at least one predetermined event." Petitioner asserts that Houser's disclosure satisfies this limitation because Houser discloses a document reviewer's double clicking, with a mouse, on the embedded security object to actuate <Scrutinize Signature> processing, which displays a window providing several items of security information, including the name of the signator, date and time the security information was embedded, serial number and hash value. Pet. 48–49 (citing Ex. 1005, 19:38–67). We have reviewed the cited portions of Houser and find that the disclosure supports Petitioner's assertion. The predetermined event is the double clicking on the displayed signature graphic of the security object and the activation of the security object is reflected in the revelation of additional information in the security object. The testimony of Mr. Zatkovich confirms the same. Ex. 1002 ¶ 87. We are sufficiently persuaded that Houser discloses the limitation of "further comprising activating the digital identification module in response to at least one predetermined event."

Claim 33 depends from claim 31 and recites "further comprising defining the at least one predetermined event as clicking on the primary component with a pointing device." As discussed above in the context of claim 26, Petitioner regards Houser's signature graphic or electronic chop as the primary component of the security object. *See* Pet. 40. The above analysis of claim 31 fully accounts for the limitation added by claim 33 because double clicking on the signature graphic of the security object with a mouse satisfies "clicking on the primary component with a pointing device."

Claim 34 depends from claim 31 which depends from claim 30. Claim 34 recites "further comprising revealing the at least one metadata component in response to activating the digital identification module." As discussed above in the context of claim 30, Petitioner regards Houser's "signature digest" as the metadata component. Pet. 47. Thus, the reference in claim 34 to "the at least one metadata component" must also refer to Houser's signature digest. In discussing claim 34, however, Petitioner identifies the document's hash value as the metadata. Pet. 51. The document hash value is not a part of the signature digest but is a part of the document digest. Ex. 1005, 12:42–54, 13:6–10. This discrepancy, however, is harmless, because Petitioner reproduces Figure 9B of Houser to illustrate what is displayed in response to a user's activating the security object. Pet. 51. Figure 9B of Houser is reproduced below:

FIG. 9B



Scrutinize Signature [Info]

Signator: James M. Adler

File Name: file3.doc

Date: 9/01/1994

Dotted Line Version: 1.0

Path: c:\user\jma

Time of Insertion: 12:48:42

File Hash Value: 7243

Serial Number: 20030.

Signature Graphic:

Comments: Authorize payment of $1,000,000 to US Olympic Team

Figure 9B illustrates the display screen in conjunction with the <Scrutinize Signature> feature of Houser. Ex. 1005, 7:3–5.

As shown in Houser's Figure 9B, the items displayed when the security object is activated by way of the <Scrutinize Signature> feature include the name of the signator, the date and time the security object was embedded, and a serial number, all of which are a part of the signature digest. *Id.* at 13:10–14. Accordingly, based on the evidence presented by Petitioner, Petitioner has made an adequate showing that Houser discloses the limitation of "further comprising revealing the at least one metadata component in response to activating the digital identification module."

For the foregoing reasons, Petitioner has shown a reasonable likelihood that it would prevail in establishing that each of claims 27, 30, 31, 33, and 34 is anticipated by Houser.

7. Dependent Claims 28, 29, 35, and 36

Claim 28 depends from claim 26 and recites "further comprising defining receiving at least one verification data element from the entity as receiving at least one unique identification number from the entity." Petitioner points to disclosure in Houser that "a private key and/or a public key pair may be entered by the user to encrypt information stored with the electronic document security application and/or information embedded into an electronic document." Pet. 45 (citing Ex. 1005, 9:36–60). Specifically, Petitioner regards "a public key and/or a private key" as the claimed *unique identification number*. *Id.* Petitioner's position has not been adequately explained. For instance, Petitioner does not explain what is *identified* by either a public key or a private key, or by a public key and a private key pair, much less why any of those items constitutes a "unique" number. The cited testimony of Mr. Zatkovich also provides no explanation on that point. Ex. 1002 ¶ 80. Accordingly, Petitioner has not made an adequate showing that Houser discloses the limitation of "further comprising defining receiving at least one verification data element from the entity as receiving at least one unique identification number from the entity."

Claim 29 depends from claim 26 and recites "further comprising verifying the at least one verification data element." In the context of claim 26, as discussed above, Petitioner has identified the at least one data verification element as "password, system identification." Pet. 38. The reference in claim 29 to "the at least one verification data element" has to refer to the same information, i.e., password or system identification information. Yet, in analyzing claim 29, Petitioner discusses "name of signator" as the at least one verification data element. The discrepancy undermines the analysis and makes the analysis misdirected. Even if the discrepancy is ignored, Petitioner only explains how, in Houser, the name of the signator would be revealed by the user's opening of the Scrutinize Signature window. Pet. 46–47. Petitioner inadequately explains how displaying the name of the signator constitutes verifying the name of the signator. Accordingly, Petitioner has not made an adequate showing that Houser discloses the limitation of "further comprising verifying the at least one verification data element."

Claim 35 depends from claim 30 and recites "further comprising communicating at least one reference code to a third party." The Specification of the '860 patent does not define what constitutes a "third party." However, the Specification does describe the following: "In addition, a user, such as the recipient of the electronic document may communicate a reference code to a third party . . . ." Ex. 1001, 8:48–50.

Petitioner, in analyzing claim 35, asserts that the limitation added by claim 35 is met by Houser because Houser discloses a step of communicating a public key to a document receiver. Pet. 52. Petitioner, however, has not explained adequately why Houser's "document receiver" constitutes "a third party," particularly in light of the description in Houser that a recipient of the electronic document may communicate a reference code to a third party. *See* Ex. 1001, 8:48–50. Additionally, although we agree that a public key is a code, Petitioner has not explained why a public key for encryption purposes constitutes a "*reference* code."[6] Accordingly, based on the evidence presented by Petitioner, Petitioner has not made an adequate showing that Houser discloses the limitation of "further comprising communicating at least one reference code to a third party."

Claim 36 depends from claim 35 and recites "further comprising revealing the at least one metadata component in response to communicating at least one reference code to a third party." Because claim 36 depends from claim 35, claim 36 includes all the limitations of claim 35. 35 U.S.C. § 112, 4th Paragraph. The deficiency of the Petition with respect to claim 35, as discussed above, carries through to claim 36.

C. Alleged Obviousness of Claims 32 and 37 over Houser and Mansz

1. Mansz

Mansz is directed to information authentication and associated feedback provided to users. Ex. 1007 ¶ 1. Mansz explains that verifying valid web sites and email messages has become very difficult to computer users. *Id.* ¶ 2. One of Mansz's disclosed embodiments refers to a "document," which Mansz regards as including a web page or an email message. *Id.* ¶ 51. In an embodiment treating a web page as a document, Mansz describes the following:

> In one embodiment of the present invention, the document (123) can have a trust mark (125). When the document is loaded into the active document browser process (121) on the user

[6] In that regard, the '860 patent describes the following: "[I]t is contemplated that the reference codes may be communicated to the module generating assembly 50, or other third party, such as, for example a web site, and gather more information about the entity 30 or the particular digital identification module." Ex. 1001, 6:65–7:2.

> device (119). The trust mark (125) is detectable by the background security process (133) running on the user device (119).

Id. ¶ 52.

> In one embodiment of the present invention, the background security process (133) verifies the authenticity of the document (123) using the trust mark (125), based on the security configuration data (131) on the user device (119).

Id. ¶ 54.

In particular, "the verification process is started when the cursor hovers over the representation of the trust mark." *Id.* ¶ 96. Mansz explains:

> In one embodiment of the invention, a background application process detects when a user places their mouse over a representation of a trust mark (e.g., an icon or a hyperlink). The background application verifies the validity of the encrypted data of the trust mark in response to the mouse over event on the trust mark.

Id. ¶ 97.

2. Claims 32 and 37

Claim 32 depends from claim 31 and recites "further comprising defining the at least one predetermined event as hovering a pointing device over the primary component." We already have discussed above, in the context of claim 31, how Houser discloses double clicking on its signature graphic to activate <Scrutinize Signature> processing, and we determined that Houser's double clicking on the signature graphic is the predetermined event. To satisfy claim 32, however, the predetermined event has to be hovering the mouse over the signature graphic, not double clicking.

Petitioner asserts that it would have been obvious to one with ordinary skill in the art to combine the digital verification system of Houser with the mouse-over feature of Mansz. Pet. 59. According to Petitioner, the hovering of a pointing device over a target as required by claim 32 was commonly known, at the time of the ’860 invention, as a “mouse over.” Pet. 56 (citing Ex. 1002 ¶ 128.). Mr. Zatkovich testifies that “[a]s Mansz confirmed, mouse overs were well known and commonly used as an alternative to key strokes, clicks, and double clicks in the context of computer systems, at the time the ’860 Patent was filed.” Ex. 1002 ¶ 129, *cited in* Pet. 56. Mr. Zatkovich further testifies the following:

> In my experience, the mouse over technique described in Mansz was well known at the time as a method to receive additional information about an object or link in a small pop up window. It could also serve as an alternative to clicking or double click on an object in an electronic environment, such as a Windows browser, in order to display information about that object.

Ex. 1002 ¶ 140, *cited in* Pet. 56. Mr. Zatkovich explains that “[i]n fact, the primary purpose of a ‘mouse over’ is to reveal additional information, such as metadata, about an object or hyperlink using a pop-up display (like the ‘Scrutinize Signature’ displays taught in [Houser]) so that the user does not have to leave the context of the current display to see the information.” Ex. 1002 ¶ 131, *cited in* Pet. 56.

Petitioner also explains the following:

> Specifically, Houser discloses revealing metadata components relating to an embedded security object when a user double-clicks on the object, or it “may be invoked by other known techniques.” (Ex1005, 19:38–52). In fact, just as in Mansz, a user of Houser’s system can use a mouse event to invoke a process for verifying the authenticity of security object (e.g., “Scrutinize Signature”). (*Id.*).
>
> Thus, by 2008, a POSITA would have known that the mouse-over event of Mansz could be used in the system of Houser as another known technique in order to invoke the

> <Scrutinize Signature> authentication process, or simply to allow metadata to be revealed without having to "click" on the security object.

Pet. 61. Petitioner further explains that "[b]y 2008, a POSITA would have been motivated to combine Houser's system with the mouse-over feature of Mansz to improve the system of Houser and to make it easier to use." *Id.* at 62. Petitioner's explanations are supported by the testimony of Mr. Zatkovich. *See* Ex. 1002 ¶¶ 140, 160–162. For instance, Mr. Zatkovich testifies as follows:

> For example, the mouse-over feature improves the user interface of the Houser system by allowing the user to view the metadata of the digital identification module simply by mousing-over the displayed module to reveal the metadata in a pop-up window. This would be instead of other alternative methods such as clicking on the identification module which would invariably change the display in order to reveal the metadata.

Id. ¶ 161.

Based on the foregoing, we determine that Petitioner has articulated reasoning with rational underpinning on why one with ordinary skill in the art would have modified Houser's double clicking to Mansz's mouse-over feature to activate Houser's security object to obtain additional information.

Claim 37 depends from claim 32 and recites "further comprising pre-selecting the electronic file." Petitioner cites to the following disclosure of Houser: "After the document is created, an electronic document security application 120 may be used to embed a security object in the electronic document as represented at 130." Ex. 1005, 7:29–31, *quoted in* Pet. 65. We are sufficiently persuaded that the portion of Houser cited by Petitioner meets the claim requirement of "pre-selecting the electronic file" because the electronic file is first created in its entirety and then the security object is embedded.

For the foregoing reasons, Petitioner has shown a reasonable likelihood that it would prevail in establishing that each of claims 32 and 37 would have been obvious over Houser and Mansz.

D. Alleged Obviousness of Claim 38 over Houser, Mansz, and Gupta

1. Gupta

Gupta discloses a software tool for digitally signing multiple documents. Ex. 1011, Abstr. Gupta describes "[w]hen a user wishes to sign multiple documents containing embedded executable code for purposes of authenticating the code, the user launches the software tool." *Id., quoted in* Pet. 66. Gupta further states that "[t]he user specifies the documents which he or she wishes signed. Thereupon, the tool automatically signs each of the documents and displays the results." Ex. 1011, Abstr.

In particular, Gupta describes the following:

> Thus, the signing tool can be launched once to sign any number of documents. The user can specify a single, hundreds, or even thousands of documents which need to be signed. The signing tool then automatically generates the digital signatures for signing the software embedded in each of the documents. This highly automated process is much more efficient and less labor intensive than requiring a user to execute a software program to sign a single document and then having the user re-execute that software program to sign another document and then having the user repeatedly execute the software program to separately sign each document on an individual basis.

Id. 3:16–27, *quoted in* Pet. 67.

2. Claim 38

Claim 38 depends from claim 32 and recites "further comprising pre-selecting a number of electronic files." As explained above, the limitations of claim 32 are met by the combined teachings of Houser and Mansz. Petitioner relies on Gupta to meet the extension of pre-selecting a single file to pre-selecting multiple files as required by claim 38.

Petitioner explains the following, with respect to Gupta:

> As shown in Figure 1 (below), a user initially **specifies** one or more documents ("files") to be digitally signed. ([Ex. 1011], Figure 1, step 101, 2:54–61). The user then specifies an appropriate certificate which is accessed and used to generate digital signatures for the software embedded in each of the documents. Gupta teaches that the certificate is accessed repeatedly to generate digital signatures until all of the documents are digitally signed. (*Id.*, Figure 1, steps 102–105, 3:3–13). In other words, each digital signature is matched with the corresponding document that was specified prior to creating the digital signature, such that the digital signature is usable with the document (electronic file).

Pet. 66–67. The explanation is supported by the cited disclosure of Gupta.

Petitioner asserts that it would have been obvious to one with ordinary skill in the art to include the step of pre-selecting a number of electronic files, as taught by Gupta, in the digital identification method disclosed by Houser. *Id.* at 68 (citing Ex. 1002 ¶ 249). Petitioner explains that Houser, Mansz, and Gupta are all directed to protecting digital documents using digital signature, and Petitioner specifically identifies Gupta's disclosure of automatically signing multiple pre-generated documents as being more efficient and less labor intensive than separately signing each document. *Id.* at 69 (citing Ex. 1011, 3:16–27).

Petitioner explains that one with ordinary skill in the art would have been motivated to use Gupta's software in Houser's electronic document verification system to sign multiple documents to improve efficiency. *Id.* at 69–70. Based on the evidence presented by Petitioner, we find that Petitioner has articulated reasoning with rational underpinning as to why one with ordinary skill in the art would have applied Gupta's teaching, about signing multiple pre-selected documents, in Houser's system and method.

For the foregoing reasons, Petitioner has shown a reasonable likelihood that it would prevail in establishing that claim 38 would have been obvious over Houser, Mansz, and Gupta.

III. CONCLUSION

On April 24, 2018, the Supreme Court held that a final written decision under 35 U.S.C. § 318(a) must decide the patentability of all claims challenged in the petition. *SAS Inst., Inc. v. Iancu*, 138 S. Ct. 1348, 1359–60 (2018). After considering the evidence and arguments presented in the Petition, we determine that Petitioner has shown a reasonable likelihood that it would prevail in establishing the unpatentability of claims 26, 27, 30–34, 37, and 38 of the '860 patent. We question, however, the sufficiency of Petitioner's contentions with respect to claims 23–25, 28, 29, 35, 36, and 39, as discussed above. We nevertheless institute an *inter partes* review of all challenged claims on all asserted grounds.

No final determination has yet been made with regard to the patentability of any claim.

IV. ORDER

It is

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review of claims 23–39 of the ’860 patent is instituted, and that the specific grounds of unpatenbtability, directed to specific claims, are all of those listed in the table presented above; and

FURTHER ORDERED that, pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4(b), *inter partes* review of the ’860 patent shall commence on the entry date of this Order, and notice is hereby given of the institution of a trial.

FOR PETITIONER:

Charles R. Macedo
Mark Berkowitz
AMSTER, ROTHSTEIN & BERNSTEIN LLP
emacedo@arelaw.com
mberkowitz@arelaw.com

FOR PATENT OWNER:

Eugenio J. Turres-Oyola
Jean Vidal-Font
Victor M. Rodriguez-Reyes
Rafael Rodriguez-Muriel
FERRAIUOLI LLC
etorres@ferraiuoli.com
jvidal@ferraiuoli.com
vrodriguezreyes@ferraiuoli.com
rrodriguez@ferraiuoli.com