Trials@uspto.gov
571-272-7822

Paper 9
Entered: June 22, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

T. ROWE PRICE INVESTMENT SERVICES, INC.,
Petitioner,

v.

SECURE AXCESS, LLC,
Patent Owner.

Case CBM2015-00027
Patent 7,631,191 B2

Before BARBARA A. BENOIT, TRENTON A. WARD, and GEORGIANNA W. BRADEN, *Administrative Patent Judges*.

BENOIT, *Administrative Patent Judge*.

DECISION
Institution of Covered Business Method Patent Review
37 C.F.R. § 42.208

I. INTRODUCTION

T. Rowe Price Investment Services, Inc. ("T. Rowe Price" or "Petitioner") filed a Petition (Paper 1, "Pet.") requesting institution of a covered business method patent review of claims 1–5, 16, and 29–32 of U.S. Patent No. 7,631,191 B2 (Ex. 1001, "the '191 patent"). Pet. 1. T. Rowe Price is one of about 50 financial services companies charged with infringement of the '191 patent by Patent Owner Secure Axcess, LLC. Pet. 12. Secure Axcess, LLC filed a Preliminary Response ("Prelim. Resp."). Paper 8.

For the reasons that follow, we determine that the '191 patent qualifies as a covered business method patent for purposes of section 18(d)(1) of the Leahy-Smith America Invents Act ("AIA"), Pub. L. No. 112–29, 125 Stat. 284, 331. We further determine that the information presented in the Petition demonstrates that it is more likely than not that at least one claim of the '191 patent is unpatentable. Accordingly, we institute a covered business method patent review of claims 1–5, 16, and 29–32. *See* 35 U.S.C. § 324(a).

A. Related Matters

Petitioner represents that the '191 patent has been asserted against it in *Secure Axcess, LLC v. T. Rowe Price Investment Services, Inc.*, Case No. 6:13-cv-00787 (E.D. Tex). Pet. 78; *see also* Paper 6 (Patent Owner's Notice of Related Matters). Petitioner also identifies seventeen other court proceedings in which Patent Owner has asserted the '191 patent. *See* Pet. 2–3; *see* Paper 6 (Patent Owner's Mandatory Notice).

The Board instituted, on September 9, 2014, a covered business method patent review of claims 1–32 of the '191 patent (*PNC Bank, N.A. v. Secure Axcess, LLC*, Case CBM2014-00100 (PTAB September 9, 2014) (Paper 10) and an *inter partes* review of claims 1–23 and 25–32 of the '191 patent (*EMC Corp. v. Secure Axcess, LLC*, Case IPR2014–00475 (PTAB September 9, 2014) (Paper 10). The Board also instituted, on April 13, 2015, another covered business method patent review of claims 1–32 of the '191 patent (*Bank of the West v. Secure Axcess, LLC*, Case CBM2015-00009 (PTAB May 13, 2015) (Paper 21)), which was then consolidated with CBM2014-00100. *See* CBM2015-00009 (Paper 27) (Decision on Petitioners' Unopposed Joint Motion for Consolidation). An additional request for a covered business method patent review of the '191 patent has been filed and a determination whether to institute has not yet been made — *PNC Bank, N.A. v. Secure Axcess,* Case CBM2015–00039 (PTAB January 21, 2015) (Paper 6).

Considering the particular circumstances of this case, we address the merits of the Petition and do not exercise our discretion under 35 U.S.C. § 325(d) (indicating "if another proceeding or matter involving the patent is before the Office, the Director *may* determine the manner in which the post-grant review or other processing or matter may proceed . . . and may take into account whether, and reject the petition or request because, the same or substantially the same prior art or arguments previously were presented to the Office"). Petitioner is not a party to any of the instituted proceedings. *See* CBM2015-00009, Paper 27, 2 (identifying the parties involved in the

CBM2014-00100 and CBM2015-00009); IPR2014-00475, Paper 10, 2 (identifying parties). In addition, this Petition raises new issues, including asserting anticipation by a reference not at issue in the instituted proceedings and asserting that certain claims of the '191 patent fail to satisfy the written description requirement of 35 U.S.C. § 112. Pet. 77.

B. The '191 Patent

The '191 patent relates to authenticating a web page, such as "www.bigbank.com." Ex. 1001, Abstract, 1:16–18, 1:28–34. The '191 patent explains that customers can be deceived by web pages that appear to be authentic, but are not. *See id.* at 1:28–34. A web page that has been authenticated according to the techniques described by the '191 patent includes "all of the information in the same format as the non-authenticated page." *Id.* at 2:58-60. The authenticated web page, however, also includes an "authenticity stamp." *Id.* at 2:59–60.

Figures 1 and 2 are set forth below:

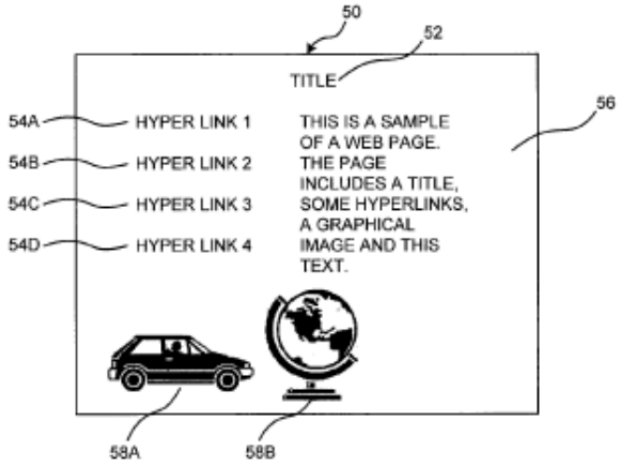


Figure 1

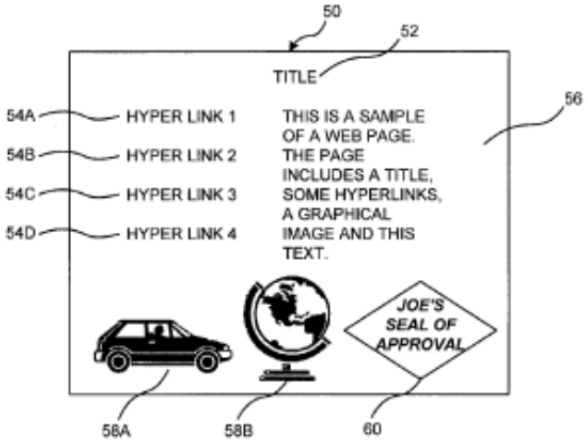


Figure 2

Each of Figures 1 and 2 shows web page 50, having title 52, hyperlinks 54A, 54B, 54C, and 54D, textual information 56, and graphical images 58A and 58B. *Id.* at 2:54–57. Figure 1 shows web page 50 has not been authenticated, whereas Figure 2 shows web page 50 has been authenticated. *Id.* at 2:54–61. The authenticated web page shown in Figure 2, unlike the non-authenticated web page shown in Figure 1, includes authenticity stamp 60. *Id.*

C. Illustrative Claims

Petitioner challenges claims 1–5, 16, and 29–32 of the '191 patent. Of the challenged claims, claims 1, 29, 31, and 32 are independent claims. Claims 1 and 29 are illustrative of the claims at issue and read as follows:

> 1. A method comprising:
>
> transforming, at an authentication host computer, received data by inserting an authenticity key to create formatted data; and

returning, from the authentication host computer, the formatted data to enable the authenticity key to be retrieved from the formatted data and to locate a preferences file,

wherein an authenticity stamp is retrieved from the preferences file.

29. An authentication system comprising:

an authentication processor configured to send formatted data having an authenticity key to a client, wherein the authenticity key enables location of a preferences file, and wherein an authenticity stamp is retrieved from the preferences file.

D. Asserted Grounds of Unpatentability

The information presented in the Petition sets forth Petitioner's contentions of unpatentability of claims 1–5, 16, and 29–32 of the '191 patent under 35 U.S.C. §§ 101, 102, 103, and 112, first paragraph, based on the following specific grounds:

Basis	Challenged Claims	Reference(s)
§ 101	1–5, 16, and 29–32	
§ 112	1–5, 16, and 32	
§ 102	1, 3, 5, 16, and 29–32	Houser[1]
§ 103	2 and 4	Houser and Yoshiura[2]

[1] U.S. Patent No. 5,606,609, issued Feb. 25, 1997 (Ex. 1004) ("Houser").
[2] European Patent Application Publication Number EP 0 883 284 A2, published Dec. 9, 1998 (Ex. 1005) ("Yoshiura").

II. ANALYSIS

A ground of unpatentability can be instituted only if the petition supporting the ground demonstrates that it is more likely than not that at least one challenged claim is unpatentable. 35 U.S.C. § 324(a); 37 C.F.R. § 42.208(c). In the analysis that follows, we discuss facts as they have been presented thus far in this proceeding. Any inferences or conclusions drawn from those facts are neither final nor dispositive of any issue related to any ground on which we institute review.

A. Claim Construction

We begin our analysis with claim construction. In a covered business method patent 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. § 42.300(b); *cf. In re Cuozzo Speed Techs., LLC,* 778 F.3d 1271, 1279–83 (Fed. Cir. 2015) ("In considering the broadest reasonable interpretation standard for *inter partes* reviews, the Federal Circuit determined that Congress implicitly adopted the broadest reasonable interpretation standard in enacting the AIA," and "the standard was properly adopted by PTO regulation."). Under the broadest reasonable construction standard, claim terms are given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art in the context of the entire disclosure. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007).

The parties submit proposed constructions for several different claim terms. Pet. 16–27; Prelim. Resp. 8–26. For purposes of this decision, we

construe "transforming" (or "transforms"); "received data"; and "authenticity key" "to locate a preferences file." No other terms in the challenged claims require express construction for this decision.

1. "transforming" or "transforms"

Independent claim 1 recites "transforming, at an authentication host computer, received data by inserting an authenticity key to create formatted data."[3] Independent claim 32 recites "transforms the received data by inserting an authenticity key to create the formatted data."

Petitioner asserts the broadest reasonable construction of "transforming" is "formatting" and the broadest reasonable construction of "transforms" is "formats." Pet. 24–25. Petitioner indicates that the term "transform" does not appear in the written description of the '191 patent. *Id.* Petitioner further relies on the testimony of its declarant Mr. Bruce Schneier that the construction of "transforming" to mean "formatting" finds support in the written description of the '191 patent. *Id.* at 26–27 (citing Ex. 1008 ¶¶ 38–43).

In contrast, Patent Owner contends "transforming" means "changing." Prelim. Resp. 24. Patent Owner supports its contention with a general purpose dictionary definition. *Id.* Patent Owner further relies on the language in claims 1, 10, and 13 that indicates how the transformation

[3] Although claims 10 and 13 are not challenged in this Petition, those claims respectively recite, similarly to claim 1, "further transforming received data by inserting a second authenticity key into the received data" and "further transforming by inserting a second authenticity key into the formatted data."

occurs—by inserting an authenticity key. *Id.* at 25. Because the written description describes inserting an authenticity key, Patent Owner contends that the written description of the '191 patent is consistent with its proposed construction of "transforming" as "changing." *Id.* at 25–26 (citing Ex. 1001, 1:55–57, 7:64–8:6).

We agree with Petitioner's proposed construction. The language of independent claims 1 and 32 each recites the result of transformation—"transforming . . . to create formatted data" and "transforms . . . to create the formatted data." Further, as indicated by Petitioner's declarant Mr. Schneier, the written description of the '191 patent does not describe expressly "transforming" but expressly describes "a formatting step to create formatted data, *i.e.*, the web page." Ex. 1008 ¶ 40; *see* Ex. 1001, 5:4–6 ("The logic of retrieving and formatting the requested page is described below with reference to FIGS. 9 and 10."). Being mindful not to import limitations from the Specification into the claims, we agree that the Specification is consistent with construing "transform" to mean "format."

On this record, we are persuaded the result of the recited transformation—formatted data—stays true to the claim language and most naturally aligns with the Specification's description of the invention. *See Translogic Tech.*, 504 F.3d at 1257 ("The specification 'is the single best guide to the meaning of a disputed term.'") (quoting *Phillips v. AWH Corp.*, 415 F.3d 1303, 1315 (Fed. Cir. 2005) (en banc)); *cf. Phillips*, 415 F.3d at 1316 ("The construction that stays true to the claim language and most naturally aligns with the patent's description of the invention will be, in the

end, the correct construction.") (citation omitted). Further, the dependent claims do not have any language that would indicate a different construction.

Accordingly, on this record, we are persuaded that the broadest reasonable construction of "transforming" (or "transforms"), in light of the Specification of the '191 patent, is "formatting" (or "formats").

2. "received data"

Independent claim 1 recites "transforming, at an authentication host computer, received data by inserting an authenticity key to create formatted data." Neither Petitioner nor Patent Owner proposes an express construction for "received data," as recited in claim 1. As made clear by Patent Owner's arguments concerning the asserted prior art, however, Patent Owner contends that "received data," as recited in claim 1, is limited to data received by the authentication host computer and "sent from elsewhere"—presumably, a device other than the authentication host computer. Prelim. Resp. 39.

Claim 1 does not recite expressly from where the received data originates. Moreover, Patent Owner has not provided sufficient evidence at this juncture to persuade us that "received data" recited in claim 1 is limited to data sent from a device other than the authentication host computer. Thus, the broadest reasonable construction of "received data" encompasses receiving data sent from a component in or associated with the authentication host computer.

3. "authenticity key" "to locate a preferences file"

Each of the independent claims recites some limitation regarding the authenticity key and locating a preferences file. Independent claim 1 recites "the formatted data to enable the authenticity key . . . to locate a preferences file." Independent claim 29 recites "the authenticity key enables location of a preferences file." Independent claim 31 recites "the authenticity key is retrieved from the formatted data to locate a preferences file." Independent claim 32 recites "retrieving, by the client computer, the authenticity key from the formatted data to locate a preferences file."

As made clear by Patent Owner's construction arguments for other limitations and its arguments regarding an asserted prior art reference, Patent Owner contends that the claims require the preferences file containing the authenticity stamp to be hidden. *See, e.g.*, Prelim. Resp. 22, 32 (indicating "the preferences file containing the authenticity stamps is hidden"), 46 (asserting the prior art reference "cannot possibly disclose [the recited] authenticity key that provides the ability to determine the location of a preferences file because [the component asserted to disclose to the recited preferences file] is not hidden"). In support of its position, Patent Owner relies on a preferred embodiment disclosed in the written description in which the preferences file is hidden and its location is determined only after the authenticity key is verified. Prelim. Resp. 21–22 (citing Ex. 1001, 4:37–38, 4:16–25, 9:53–57).

We acknowledge that the written description indicates "[p]referably, the preferences file is placed in a random directory to help obscure the

location of the preference file and facilitate the creation of unique user configurations." Ex. 1001, 9:53–57. Independent claims 1, 29, 31, and 32, however, do not recite expressly that the preferences file location is obscured or hidden. We decline to read limitations into a claim even from a preferred embodiment described in the Specification if the claim language is broader than the embodiment. *In re Am. Acad. of Sci. Tech Ctr*., 367 F.3d 1359, 1364 (Fed. Cir. 2004). *In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993). Here, none of the claims requires that the preferences file is placed in a particular location or in a particular way. Thus, the claim language is broader than the preferred embodiment that describes the preferences file is placed in a random directory to help obscure the location of the preferences file.

Accordingly, on this record, we are not persuaded by Patent Owner's argument that the claims require the preferences file be hidden.

B. Standing

Section 18 of the AIA provides for the creation of a transitional program for reviewing covered business method patents. Section 18 limits reviews to persons or their privies who have been sued or charged with infringement of a "covered business method patent." AIA § 18(a)(1)(B); *see* 37 C.F.R. § 42.302. As discussed above in Section I.A., Petitioner represents it has been sued for infringement of the '191 patent and is not estopped from challenging the claims on the grounds identified in the Petition. Pet. 4, 78; *see* Paper 6 (Patent Owner's Mandatory Notice).

The parties dispute whether the '191 patent is a "covered business method patent," as defined in the AIA and 37 C.F.R. § 42.301. *See* Pet. 9 – 15; Prelim. Resp. 26–42. "[T]he term 'covered business method patent' means a patent that claims a method or corresponding apparatus for performing data processing or other operations used in the practice, administration, or management of a financial product or service, except that the term does not include patents for technological inventions." AIA § 18(d)(1); *see* 37 C.F.R. § 42.301(a).

We conclude that the '191 patent meets the definition of a "covered business method patent" for the reasons set forth below, and that Petitioner has standing to file a petition for a covered business method patent review.

1. Financial Product or Service

One requirement of a covered business method patent is for the patent to "claim[] a method or corresponding apparatus for performing data processing or other operations used in the practice, administration, or management of a financial product or service." AIA § 18(d)(1); *see* 37 C.F.R. § 42.301(a). The legislative history of the AIA "explains that the definition of covered business method patent was drafted to encompass patents 'claiming activities that are financial in nature, incidental to a financial activity or complementary to a financial activity.'" 77 Fed. Reg. 48,374, 48,735 (Aug. 14, 2012) (quoting Cong. Rec. S5432 (daily ed. Sept. 8, 2011)). The legislative history of the AIA further indicates that the language "practice, administration and management" of a financial product or service "is intended to cover any ancillary activities related to a financial

product or service, including, without limitation, marketing, customer interfaces, Web site management and functionality, transmission or management of data, servicing, underwriting, customer communications, and back office operations—e.g., payment processing, stock clearing." 157 Cong. Rec. S1364–65 (daily ed. Mar. 8, 2011) (statement of Sen. Schumer).

Petitioner contends the '191 patent meets the financial product or service requirement because the claims are directed to performing data processing used in the administration of a financial product or service. Pet. 10–12. Specifically, Petitioner indicates that the '191 patent relates to authenticating web pages in an electronic commerce system for exchanging data or transacting business and facilitating online commerce transactions between a customer and a bank. *Id.* at 11 (citing Ex. 1001, 1:16–18, 1:33, 8:21–23, 11:1–2, 11:30–31, 11:60–67). Petitioner also notes that Patent Owner has sued approximately fifty financial institutions, including banks. *Id.* at 12.

In response, Patent Owner contends that financial products and services include "only financial products such as credit, loans, real estate transactions, check cashing and processing, financial services and instruments, and securities and investment products." Prelim. Resp. 28; *see generally id.* at 26–29. According to Patent Owner, the '191 patent claims an authentication server that authenticates data (such as a web page) from a server. *Id*. at 33. As such, Patent Owner contends the '191 patent is not a covered business method patent, because (1) the claimed method and apparatus is directed to techniques to distinguish authenticated data, (2) none

of the claims mentions a financial product or service, and (3) the claimed method and apparatus aid businesses in general. *Id*. at 30–33, 35. Patent Owner further contends that asserting the '191 patent against financial institutions is not sufficient to demonstrate the '191 patent is directed to a financial product or service. *Id.* at 33–35. Patent Owner also indicates that the '191 patent has been asserted against financial institutions because of the manner in which they authenticate web pages and that companies other than financial institutions allegedly practice the techniques claimed by the '191 patent. *Id.* at 34.

Based on the record before us, we determine that the method and apparatus claimed by the '191 patent perform operations used in the administration of a financial product or service and are incidental to a financial activity. The written description of the '191 patent discloses a need by financial institutions to ensure customers are confident that the financial institution's web page is authentic (Ex. 1001, 1:28–33); alternative embodiments of the invention are disclosed as being used by financial institutions (*id.* at 8:21–23, 11:23–40, 11:52–67) and used in commerce, including (i) transacting business over a network, such as the Internet (*id.* at 10:65–11:3); and (ii) selling goods, services, or information over a network (*id.* at 11:17–21).

The '191 patent relates to authenticating a web page and claims a particular manner of doing so— by inserting an authenticity key to create formatted data, enabling a particular type of computer file to be located, from which an authenticity stamp is retrieved. Ex. 1001, 1:16–18, 12:9–18.

The ’191 patent is directed to solving problems related to providing a web site to customers of financial institutions. Thus, the ’191 patent covers the ancillary activity related to a financial product or service of Web site management and functionality and so, according to the legislative history of the AIA, the method and apparatus of the ’191 patent perform operations used in the administration of a financial product or service.

Although not determinative, Patent Owner’s many suits alleging infringement of claims of the ’191 patent by financial institutions is a factor weighing toward the conclusion that the ’191 patent claims a method or apparatus that at least is incidental to a financial activity, even if other types of companies also practice the claimed invention. Pet. 12.

Therefore, the ’191 patent claims a method or corresponding apparatus for performing data processing or other operations used in the practice, administration, or management of a financial product or service. *See* 37 C.F.R. § 42.301(a).

2. Exclusion for Technological Inventions

The definition of “covered business method patent” in Section 18 of the AIA expressly excludes patents for “technological inventions.” AIA § 18(d)(1); *see* 37 C.F.R. § 42.301(a). To determine whether a patent is for a technological invention, we consider “whether the claimed subject matter as a whole recites a technological feature that is novel and unobvious over the prior art; and solves a technical problem using a technical solution.” 37 C.F.R. § 42.301(b). The following claim drafting techniques, for example, typically do not render a patent a “technological invention”:

> (a) Mere recitation of known technologies, such as computer hardware, communication or computer networks, software, memory, computer-readable storage medium, scanners, display devices or databases, or specialized machines, such as an ATM or point of sale device.
>
> (b) Reciting the use of known prior art technology to accomplish a process or method, even if that process or method is novel and non-obvious.
>
> (c) Combining prior art structures to achieve the normal, expected, or predictable result of that combination.

Office Patent Trial Practice Guide, 77 Fed. Reg. 48,756, 48,764 (Aug. 14, 2012).

Petitioner indicates that the '191 patent is not directed to a technological invention, because the '191 patent does not claim a novel, nonobvious technological feature and does not solve a technical problem using a technical solution. Pet. 13–15. As noted by Petitioner, the claims recite only known computer components and do not claim specialized technology, such as encryption algorithms, for authenticating a web page. *Id.* According to Petitioner, the '191 patent is directed to solving a non-technical problem—ensuring customers are confident that web pages are authentic. *Id.* at 15. The purported technical solution is providing a visual indication that a web page is authentic, which Petitioner contends is a non-technical solution. *Id.*

Patent Owner disagrees. Prelim. Resp. 36–42. Patent Owner contends that every claim of the '191 patent "solves the technical problem of distinguishing authentic data (e.g., data for web pages) sent by a legitimate site from fraudulent data sent by a fraudulent site." *Id.* at 36. Patent Owner

further contends the claimed subject matter, as a whole, recites a technological solution — a computer-implemented system, including an authentication system, an authentication key, and an authentication stamp — that executes a particular series of steps. *Id.* at 38.

Although the claimed steps of the '191 patent may be an allegedly novel and nonobvious process, based on the record before us, we find that the technological features of the claimed steps are directed to using known technologies. *See* 77 Fed. Reg. at 48,764 (indicating use of known technologies does not render a patent a technological invention). The Specification indicates that components of the computer system used in the claimed authentication process are known technologies. For example, the Specification discloses known computer systems and devices running known operating systems (Ex. 1001, 3:30-34, 10:30–35, 11:7–12), known user input devices (*id.* at 11:3-6), and known networks and networking and communication protocols (*id.* at 3:38–49, 10:67–11:3, 11:12–17). The Specification further discloses that the system is programmed using known programming and scripting languages, and known data structures (*id.* at 10:35–40), and discloses that the system uses "conventional techniques for data transmission, signaling, data processing, network control, and the like" (*id.* at 10:41–44).

Furthermore, the Specification describes using known cryptography techniques for encrypting and decrypting the authenticity key. *See id.* at 6:28–32. Also, the Specification incorporates by reference a cryptography text. *Id.* at 10:44–48. The recited authentication stamp is described as

having a number of variations, including graphics only, text only, text and graphics, audio, blinking (*id.* at 2:67–3:4), but does not describe novel or nonobvious technology used to implement those features.

Patent Owner has not shown persuasively that the claimed subject matter, as a whole, requires any specific, unconventional software, computer equipment, cryptography algorithms, processing capabilities, or other technological features. Patent Owner's identification of allegedly novel or unobvious steps, such as limitations in independent claim 1 and dependent claims 3 and 4 (Prelim. Resp. 37–38), does not persuade us that any of the steps require the use of specific computer hardware alleged to be novel and unobvious over the prior art. Nor are we persuaded that any of the claimed steps, the claimed instructions, or the claimed authentication system solves a technical problem using a technical solution, as Patent Owner contends (*id.* at 36, 38, 42). Reciting the use of known prior art technology to accomplish a process or method, even if that process or method is novel and non-obvious, does not render the claimed subject matter a technological invention. *See* 77 Fed. Reg. at 48,764.

Thus, we conclude the '191 patent is not directed to a technological invention, which is excluded from a covered business method patent review. Accordingly, the '191 patent is eligible for a covered business method patent review.

C. Asserted Ground that Claims 1–5, 16, and 29–32 Are Unpatentable Under § 101

Petitioner challenges claims 1–5, 16, and 29–32 of the '191 patent as being directed to patent-ineligible subject matter under 35 U.S.C. § 101. Pet. 74–77. Patent-eligible subject matter is defined in 35 U.S.C. § 101:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

There are, however, three limited, judicially-created exceptions to the broad categories of patent-eligible subject matter in § 101: laws of nature; natural phenomena; and abstract ideas. *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 132 S. Ct. 1289, 1293 (2012). The Supreme Court has made clear that the test for patent eligibility under § 101 is not amenable to bright-line categorical rules. *Bilski v. Kappos*, 561 U.S. 593, 595 (2010).

1. Whether the Claims Are Directed to an Abstract Idea

Petitioner contends the claims fall within the judicially created exception encompassing abstract ideas. Pet. 27–43. In *Alice Corp. Pty, Ltd. v. CLS Bank International*, 134 S. Ct. 2347 (2014), the Supreme Court reiterated the framework set forth previously in *Mayo*, "for distinguishing patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of these concepts." *Alice*, 134 S. Ct. at 2355. The first step in the analysis is to "determine whether the claims at issue are directed to one of those patent-ineligible concepts." *Id.* "If not, the claims pass muster under § 101." *Ultramercial, Inc. v. Hulu,*

LLC, 772 F.3d 709, 714 (Fed. Cir. 2014). If, however, the claims are directed to a patent-ineligible concept, the second step in the analysis is to consider the elements of the claims "individually and 'as an ordered combination'" to determine whether there are additional elements that "'transform the nature of the claim' into a patent-eligible application." *Alice*, 134 S. Ct. at 2355 (quoting *Mayo*, 132 S. Ct. at 1291, 1297). We must examine the claim as a whole, considering the claim elements both individually and in combination. *Alice*, 134 S. Ct. at 2355 n. 3.

Turning to the Petition, Petitioner, relying on the framework set forth in *Mayo* and followed in *Alice*, asserts that the challenged claims are unpatentable under § 101 as abstract ideas. Pet. 30–43. According to Petitioner, the claims are directed to the computerized application of the fundamental economic practice of notarizing documents and preempt the basic operation of electronic document notarization. Pet. 1–2, 30–43. Further, Petitioner contends that the challenged claims recited abstract ideas implemented using general-purpose computer components. *Id.* at 2, 27–30. Therefore, according to Petitioner, the challenged claims are patent-ineligible abstract ideas. *Id.* at 27–43.

Petitioner contends the challenge claims directly track the traditional notarization process. *Id.* at 31–36. Petitioner's position is that the act of notarizing a document verifies or authenticates the executed document and the "certificate of notarization" added by the notary at or near the end of the document functions the same way as the recited authenticity key. *Id.* at 32. Petitioner's example "certificate of notarization" is set forth below.

STATE OF _____)
)ss.
COUNTY OF _____)

On this ____ day of _____ 20___, before me, the subscriber, a Notary Public in and for said State and County, personally appeared _____, the _____ of _____, known or identified to me to be the person whose name is subscribed to the within instrument, and in due form of law acknowledged that he/she is authorized on behalf of said company to execute all documents pertaining hereto and acknowledged to me that he/she executed the same as his/her voluntary act and deed on behalf of said company.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed my seal in said State and County on the day and year last above written.

Notary Seal

_____
(Signature of Notary)

My Commission Expires: _____

Id. As shown in the example, a "certification of notarization" (once completed by the notary) includes information about the date and place of execution, as well as signatory and notary information.

Further, according to Petitioner, adding the "certificate of notarization" formats the original document into a document that is ready for authentication and so is analogous to "transforming . . . received data by inserting an authenticity key to create formatted data," as recited by claim 1. *Id.* at 32–33. Applying a notary seal to the document is analogous to the recited "authenticity stamp," and the base plates included with the notary's stamp and seal are analogous to the recited "preferences file." *Id.* at 34–35. Thus, according to Petitioner, the claimed authentication host computer solves the same problem as the traditional notarizing process. *Id.* at 36.

In determining whether a method or process claim recites an abstract idea, "we first examine the claims because the claims are the definition of what a patent is intended to cover." *Ultramercial,* 772 F.3d at 714. Claim 1, as a whole, relates to a computer-implemented method to transform data in a particular manner—by inserting an authenticity key to create formatted data, which, in turn, enables a particular type of computer file to be located and from which an authenticity stamp is retrieved.

We are not persuaded that the challenged claims are directed to the computerized application of the abstract idea of notarizing documents, notwithstanding Petitioner's strained analogy. On its face, there is nothing immediately apparent about the data processing operations recited in claim 1 to persuade us that the claim is directed to an abstract idea of notarizing documents. Unlike the information found in a "certificate of notarization," claim 1 does not recite any information about the signatory, the notary, or the execution of the document. Nor do any of the other challenged independent claims do so. Further, neither claim 1 nor any of the other challenged independent claims recites verifying the identity of the signatory or authenticity of a document.

One of the challenged dependent claims (claim 3), however, recites "verifying the authenticity of the formatted data based on the authenticity key in response to the formatted data including the authenticity key." On its face, the additional limitation recited in dependent claim 3 is not directed to the abstract idea of notarizing documents. Further, the additional limitation recited in dependent claim 3 has a degree of particularity and is tied to a

particular tangible form—verifying the authenticity of the formatted data under a particular condition and in a particular manner (that is, "based on the authenticity key in response to the formatted data including the authenticity key").

Moreover, the ordered combination of steps recited in claim 1 has a degree of particularity not found in an abstract idea. *See DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1259 (Fed. Cir. 2014) (concluding that the claims at issue "recite a specific way to automate the creation of a composite web page by an 'outsource provider' that incorporates elements from multiple sources in order to solve a problem faced by websites on the Internet"). For example, claim 1 requires transforming a type of data ("received data") in a particular manner ("by inserting an authenticity key to create a formatted data"). Claim 1 also returns the formatted data having the authenticity key from a particular location ("from the authentication host computer") for a particular purpose ("to enable the authenticity key to be retrieved from the formatted data and to locate a preferences file"). A particular item ("an authenticity stamp") is retrieved from another particular item ("the preferences file"). The steps in claim 1 also are tied to a tangible form—formatted data having an authenticity key, formatted data enabling certain actions ("to enable the authenticity key to be retrieved from the formatted data and to locate a preferences file"), and an authenticity stamp being located in a preferences file.

Furthermore, the challenged claims differ markedly from the claims at issue in *Alice*, *Bilski*, and *Ultramercial*. On their face, the claims in those

cases closely reflect their analogous abstract human activity. For example, the claims in *Alice* involved "a method of exchanging financial obligations between two parties using a third-party intermediary to mitigate settlement risk." *Alice*, 134 S. Ct. at 2356. The Court determined that the claims in *Alice* were drawn on their face to the concept of using a third party to mitigate settlement and that representative method claim 1 recited the following steps:

> (1) "creating" shadow records for each counterparty to a transaction; (2) "obtaining" start-of-day balances based on the parties' real-world accounts at exchange institutions; (3) "adjusting" the shadow records as transactions are entered, allowing only those transactions for which the parties have sufficient resources; and (4) issuing irrevocable end-of-day instructions to the exchange institutions to carry out the permitted transactions.

Alice, 134 S.Ct. at 2359.

According to the Court, the "claims at issue in *Bilski* described a method for hedging against the financial risk of price fluctuations." *Alice*, 134 S. Ct. at 2355. In *Bilski*, "[c]laim 1 recited a series of steps for hedging risk, including:

> (1) initiating a series of financial transactions between providers and consumers of a commodity; (2) identifying market participants that have a counterrisk for the same commodity; and (3) initiating a series of transactions between those market participants and the commodity provider to balance the risk position of the first series of consumer transactions."

Id. at 2355–56.

In *Ultramercial*, claim 1 included eleven steps for displaying an advertisement in exchange for access to copyrighted media:

> (1) receiving copyrighted media from a content provider; (2) selecting an ad after consulting an activity log to determine whether the ad has been played less than a certain number of times; (3) offering the media for sale on the Internet; (4) restricting public access to the media; (5) offering the media to the consumer in exchange for watching the selected ad; (6) receiving a request to view the ad from the consumer; (7) facilitating display of the ad; (8) allowing the consumer access to the media; (9) allowing the consumer access to the media if the ad is interactive; (10) updating the activity log; and (11) receiving payment from the sponsor of the ad.

Ultramercial, 772 F.3d at 714–15.

For these reasons, we are not persuaded that the challenged claims are directed to a computerized application of notarizing documents or that the underlying concept of the claims is the notarization of electronic documents. *See* Pet. 42 (asserting that the underlying concept of the claims is notarization of electronic documents). Nor do we agree that the '191 patent is directed to the same problem as traditional notarization—preventing fraud. Pet. 36–37. Rather, the '191 patent addresses a narrower problem of authenticating web pages "so that a user feels secure about the authenticity of pages displayed from Internet sites." Ex. 1001, 1:44–47. Having found the challenged claims are not directed to the computerized application of notarizing documents, we need not address whether the process of notarizing is a fundamental economic practice or whether the claims would preempt the basic practice of notarizing documents.

Petitioner also asserts that the challenged claims only recite abstract ideas implemented using general-purpose computer components and so is not patent-eligible. Pet. 27–30, 39–43. Petitioner further asserts the challenged claims amount to no more than the abstract ideas of manipulating data, transmitting data, and gathering data. *Id.* at 40–41 (citing *Digitech Image Techs., LLC v. Electronics for Imaging, Inc.*, 758 F.3d 1344, 1351 (Fed. Cir. 2014); *In re Grams*, 888 F.2d 835, 840 (Fed. Cir. 1989)).

Petitioner's reliance on *Digitech Image* and *Grams* is unpersuasive. In *Digitech Image*, the Federal Circuit held that "[w]ithout additional limitations, a process that employs mathematical algorithms to manipulate existing information to generate additional information is not patent eligible." *Digitech Image*, 758 F.3d at 1351. The claims at issue in *Digitech Image* were directed to a process for generating a device profile by generating two data sets from existing information about measurements and organizing the data into a new form—the device profile. *Id.* Federal Circuit concluded, however, that the claims at issue were to a patent-ineligible abstract idea, not merely because a mathematical algorithm was employed to manipulate existing information, but because the patent-ineligible claims did not require input from a physical device. *Id.*

Here, unlike the claims at issue in *Digitech Image*, claim 1 recites transforming, at an authentication host computer, by inserting an authenticity key to create formatted data and returning the formatted data from the host computer. Thus, claim 1 requires input from a physical device and is not merely a mathematical algorithm.

Although the Federal Circuit in *Grams* held that data gathering steps cannot make an otherwise nonstatutory claim statutory, the court did not indicate that a claim with only data gathering steps and a mathematical algorithm necessarily always would be nonstatutory and depends on the claims as a whole and the circumstances of each case. *Grams,* 888 F.2d at 840 ("Whether section 101 precludes patentability in every case where the physical step of obtaining data for the algorithm is the only other significant element in mathematical algorithm-containing claims is a question we need not answer. Analysis in that area depends on the claims as a whole and the circumstances of each case.")

Claim 1 of the '191 patent recites "transforming . . . at an authentication host computer" and "returning . . . from the authentication host computer," which are not immediately apparent as being limited to data gathering. As such, on this record, claim 1 can be distinguished from claims in *Grams*, which rely on data gathering as the recited physical steps.

Petitioner further asserts that, even if the challenged claims do not preempt the abstract concept of notarizing electronic documents, the claims preempt authenticating documents in the form of web pages. Pet. 42. Even so narrowed, we do not agree that the claims preempt all ways of authenticating web pages. Rather, the claims are limited to a particular manner that involves, among other things, inserting an authenticity key to create formatted data, which enables a particular type of computer file to be located and from which an authenticity stamp is retrieved.

For these reasons, we are not persuaded by Petitioner's assertion that claims 1–5, 16, and 29–32 are patent-ineligible abstract ideas. As such, we need not turn to the second step in the *Mayo* framework to look for additional elements that can transform the nature of the claim into a patent-eligible application of an abstract idea.

2. Whether the Claims Satisfy the Machine-or-Transformation Test

A claimed process can be patent-eligible under § 101 if "(1) it is tied to a particular machine or apparatus, or (2) it transforms a particular article into a different state or thing." *Bilski*, 545 F.3d 943, 954 (Fed. Cir. 2008) (en banc), *aff'd on other grounds, Bilski*, 561 U.S. 593. We understand that the machine-or-transformation test is a useful tool, but is not the sole test for whether an invention is a patent-eligible process under § 101. *See Bilski,* 561 U.S. at 604.

Petitioner also contends that claims 1–5, 16, and 29–32 are unpatentable under § 101, because the claims are not tied to any particular machine and transform no article into a different state or thing, and thus do not satisfy the machine-or-transformation test. Pet. 43–45. Petitioner asserts that the challenged claims recite generic computer components and do not satisfy the transformation prong of the machine-or-transformation test. Pet. 43–44. Rather, according to Petitioner, the transforming limitation in claim 1 is merely a data formatting operation, which is not patent eligible. *Id.* at 44 (citing *CyberSource Corp. v. Retail Decisions, Inc.,* 654 F.3d 1366, 1370 (Fed. Cir. 2011)). Petitioner's reliance on *CyberSource* is unpersuasive. In *CyberSource*, the Federal Circuit indicated that mere

collection and organization of data does not satisfy the transformation prong in the machine-or-transformation test. *See CyberSource*, 654 F.3d at 1370. The Federal Circuit also indicated in *CyberSource* that the mere manipulation or reorganization of data also did not satisfy the transformation prong. *See id.* at 1375. The Federal Circuit concluded, however, that the claims at issue were to a patent-ineligible abstract idea, not merely because of the collection, organization, and manipulation of data, but because all the claimed steps could be performed in the human mind, which is not the case here. *See id.* at 1373, 1376–77.

Rather, the challenged claims specifically recite "transforming . . . received data by inserting an authenticity key to create formatted data," thereby authenticating a web page with an authenticity stamp. Thus, the claims require a change to the data and a change that cannot be performed in the human mind. We are not persuaded by Petitioner that "transforming . . . received data by inserting an authenticity key to create formatted data" fails to satisfy the transformation prong. The claim language recites "transforming" one thing ("received data") "to create" something else ("formatted data") and further recites a particular manner of transforming ("by inserting an authenticity key"). The broadest reasonable construction of "transforming" is "formatting," but this construction does not alter the fact that the claim requires a particular manner of formatting—inserting an authenticity key, which provides additional data to create the formatted data—and does not merely format existing information without receiving additional input. *See Digitech Image*, 758 F.3d at 1351 (holding the claims

at issue were to a patent-ineligible abstract idea because a mathematical algorithm was employed to manipulate existing information and the claims did not require input from a physical device).

Petitioner does not provide persuasive argument or evidence for its position that the claims do not satisfy the transformation prong. Because Petitioner has not persuaded us that claim 1 does not meet the transformation prong of the machine-or-transformation test, we need not consider Petitioner's other assertions that the challenged claims do not meet the machine prong of the test. Furthermore, Petitioner does not provide further arguments regarding the other challenged claims. We, therefore, are not persuaded claims 1–5, 16, and 29–32 fail to satisfy the machine-or-transformation test.

Therefore, having considered the information provided in the Petition, as well as Patent Owner's Preliminary Response, we are not persuaded Petitioner has demonstrated that it is more likely than not that the claims challenged in the Petition are unpatentable under 35 U.S.C. § 101.

D. Asserted Ground that Claims 1–5, 16, and 32 Fail to Comply with the Written Description Requirement

Petitioner asserts that, if the terms "transforming" and "transforms" are construed to mean anything other than "formatting" and "formats," then there is no written description support for the terms "transforming" and "transforms." Pet. 50–52. For the reasons described in Section II.A., the broadest reasonable construction of "transforming" and "transforms," in light of the Specification, is "formatting" and "formats."

Accordingly, we do not institute the asserted ground that claims 1–5, 16, and 32 fail to comply with the written description requirement of 35 U.S.C. § 112.

E. Asserted Ground that Claims 1, 3, 5, 16, and 29–32 Are Anticipated By Houser

Petitioner asserts that claims 1, 3, 5, 16, and 29–32 are unpatentable under 35 U.S.C. § 102(b) as anticipated by Houser. Pet. 52–71. Petitioner provides explanations specifying where limitations of the challenged claims purportedly are disclosed in Houser. *Id.* Petitioner also relies on the declaration of Mr. Schneier (Ex. 1008). Patent Owner challenges Petitioner's assertions.

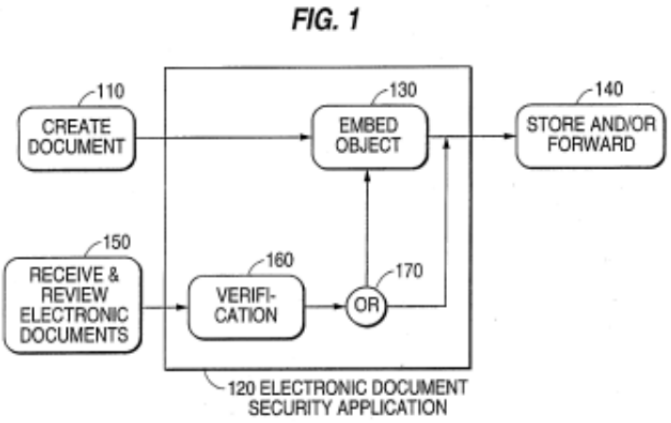
Based on the record before us, Petitioner has demonstrated that it is more likely than not that claims 1, 3, 5, 16, and 29–32 are anticipated by Houser.

1. Houser

To address the problem of altered or forged electronic documents, Houser describes techniques for indicating authenticity of an electronic document. Ex. 1004, 1:7–13, 1:59–67. More specifically, Houser describes verifying the integrity or signator of an electronic document "by embedding a security object . . . in the electronic document . . . at a location selected by the signator." *Id.* at Abstract. "The embedded security object includes security information and an identifier for invoking the processing of security information." *Id.* The security information may include "the signator's 'electronic chop,' which may be the signator's digitized signature or other

graphic image." *Id.* "If the signator and the document integrity are confirmed, the electronic chop is displayed in the document." *Id.* "If, however, the signator or document integrity are not verified, the electronic chop is not displayed." *Id.*

Figure 1 of Houser is set forth below:



The fundamental operation cycle of Houser's techniques is shown in Figure 1. *Id.* at 7:15–16. An electronic document is created at 110. *Id.* at 7:16. Then electronic security application 120 is used to embed a security object in the electronic document as represented at 130. *Id.* at 7:29–31. "The 'signed' electronic document (i.e., the electronic document including one or more embedded security objects) may be stored and/or transmitted to another party represented at 140." *Id.* at 7:62–65. The electronic document is received at 150 and an identifier in the embedded security object invokes the verification processing of the electronic document security application 120 at 160. *Id.* at 7:66–8:2. Houser indicates that performing verification processing by another electronic document security application is preferred

because it facilitates communication of electronic documents between users. *Id.* at 8:2–8.

2. Claims 1, 3, 5, and 29–32

Petitioner's Contentions

Petitioner contends each limitation of claims 1, 3, 5, and 29–32 is disclosed by Houser. For example, regarding independent claim 1, according to Petitioner, Houser's electronic document before the security object is embedded discloses the recited "received data" and the electronic document after the security object is embedded discloses the recited "formatted data." Pet. 52, 54. Petitioner's position is that Houser's graphic of the signator's digitized signature (called an "electronic chop") discloses the recited "authenticity stamp." *Id.* at 52. According to Petitioner, Houser's identifier, which is included in the security object and used to invoke the processing of security information, discloses the recited "authentication key" to be retrieved from formatted data. *Id.* at 54–55, 61.

Petitioner contends that, because the security object with the identifier is embedded in the electronic document (i.e., "the formatted data) and the identifier (i.e., "authentication key") is used to invoke the processing of security information, Houser discloses formatted data having an authentication key, as required by claim 1. *Id.* at 56, 61. Petitioner further contends that Houser's security information (which includes the "electronic chop" or other graphic, corresponding to the "authenticity stamp) in the security object discloses the recited "preferences file" from which the "authenticity stamp" is retrieved. *Id.* at 57, 64–65.

According to Petitioner, Houser's description of embedding a security object (having security information including an identifier—"authentication key") in the electronic document discloses the recited "transforming, at an authentication host computer, received data by inserting an authenticity key to create formatted data." *Id.* at 61. Petitioner contends that Houser's electronic document security application 120 implemented using a standard computer and described as embedding the security object into the electronic document discloses the recited authentication host computer. *Id.* at 59–60 (citing Ex. 1004, 7:29–31, 8:50–62).

Petitioner further contends that Houser's description of transmitting the electronic document with the embedded security object to another party and subsequently invoking the verification processing discloses the recited "returning, from the authentication host computer, the formatted data to enable the authenticity key to be retrieved from the formatted data and to locate a preferences file." *Id.* at 59–61, 63–64; *see id.* at 60 (indicating Houser's Figure 1 discloses the "'authentication host computer' (e.g., security application 120) . . . is returning or sending 'formatted data' at block 140") (citing Ex. 1004, 7:16–8:19). The portion of Houser cited by Petitioner indicates that performing verification processing by another electronic document security application is preferred because it facilitates communication of electronic documents between users. *Id.* at 60 (citing Ex. 1004, 8:2–8).

Petitioner contends that Houser's description of extracting the electronic chop ("authenticity stamp") from the embedded security object

having security information ("preferences file") and displaying the electronic chop discloses the recited "an authenticity stamp is retrieved from the preferences file." *Id.* at 64–65.

Analysis

On this record, we are persuaded by Petitioner's contentions, which have been summarized previously, regarding how Houser's elements disclose the limitations recited in independent claims 1, 29, 31, and 32, which demonstrate that Petitioner has established that it is more likely than not that the independent claims are anticipated by Houser.

Patent Owner disputes that Houser discloses a preferences file because Houser's security information is in the embedded object, which, in turn, is in an electronic document, and so the security information is not in a file, as required by the claim. Prelim. Resp. 44. Patent Owner does not provide persuasive argument as to why Houser's security information is not "a uniquely named collection of data stored on a hard drive, disk or other storage medium and treated as a single entity," which Patent Owner proposes is the broadest reasonable construction for the term "file." *Id.* at 18–19, 44.

Further, Houser refers to "security information" as a unit—"the operating system of the computer, responsive to the identifier, may invoke processing of the security information in the embedded security object." Ex. 1004, 7:35–41. Moreover, we are not persuaded that Patent Owner's

proposed construction based on a dictionary definition[4] that is after the effective filing date of the '191 patent reflects the ordinary meaning of the term "file" at the time of the invention. A technical dictionary definition that predates the effective filing date of the '191 patent provides a more general definition—"[a] collection of related records treated as a unit." MCGRAW-HILL DICTIONARY OF SCIENTIFIC AND TECHNICAL TERMS 752 (5th ed. 1994).

As noted previously, Houser treats security information as a unit, and, thus, we are not persuaded on this record that Houser's security information is not a file within the meaning of the claims of the '191 patent. Further, Houser's security information is in the security object embedded in an electronic document, which Petitioner contends meets the claim limitations regarding the recited "preferences file." Pet. 57. Houser indicates the electronic document may be "a text file." Ex. 1004, 11:52–54.

Patent Owner also contends that, because Houser's security information is not hidden, Houser does not disclose an authenticity key that provides the ability to determine a location of a preferences file. Prelim. Resp. 46. As explained in Section II.A., we are not persuaded that the location of a preferences file must be hidden and so are not persuaded by Patent Owner's contention.

Patent Owner further contends that, because the same server in Houser creates the document and embeds the security object in the

---

[4] Prelim. Resp. 18 (citing MICROSOFT ENCARTA COLLEGE DICTIONARY, THE FIRST DICTIONARY FOR THE INTERNET AGE 532 (2001) (Ex. 2006)).

document, Houser does not disclose an authentication host computer (claim 1) or a device (claims 31 and 32) receiving data sent from outside itself, as Patent Owner contends is required by claim 1. *Id.* at 47–48.

Nor are we persuaded by Patent Owner's contention that Houser does not disclose the requisite returning because Houser does not return the electronic document with the embedded security object to the application that created the electronic document. *Id.* at 48–50. Patent Owner contends that "returning" requires the formatted data to be returned to the same location from which the data was received. *Id.*

We are not persuaded, at this juncture, that independent claim 1, when read as a whole, requires returning the formatted data to the same location from which it was received. Claim 1 does not recite expressly the location to which the formatted data is returned. Furthermore, on this record, we are not persuaded by Patent Owner's arguments as to how one skilled in the art would have understood the returning limitation.

Nor are we persuaded, at this juncture, that independent claims 31 and 32 require formatted data to be sent to the client from which data was received, as Patent Owner contends (Prelim. Resp. 50–51). Claim 31 does not recite receiving data from a client but only recites "format received data," a limitation that does not specify where the received data originates. Further, claim 31 recites "to return the formatted data to *a* client" (emphasis added), a limitation that lacks an antecedent basis referring to a client recited elsewhere in the claim.

Similarly, claim 32 recites "receiving, at a client computer, formatted data from a[n] authentication host computer wherein the authentication host computer receives the data to create received data." Claim 32 recites that the formatted data is received at a client computer. Claim 32, however, does not recite expressly from where the authentication host computer receives its data, much less expressly requiring the authentication host computer to receive its data from the client computer that receives the formatted data, as proposed by Patent Owner (Prelim. Resp. 50–51).

Thus, based on the record before us, we determine the information in the Petition demonstrates that it is more likely than not that claims 1, 3, 5, and 29–32 are anticipated by Houser.

3. Dependent Claim 16

Claim 16, which depends from independent claim 1, additionally recites "the returning includes returning the formatted data to at least one of: a Personal Computer (PC), Personal Digital Assistant (PDA), cellular telephone, or an email device."

As described previously, Petitioner contends that Houser's description of transmitting the electronic document with the embedded security object to another party and subsequent invoking the verification processing discloses the recited "returning, from the authentication host computer, the formatted data to enable the authenticity key to be retrieved from the formatted data and to locate a preferences file." Pet. 60 (citing Ex. 1004, 7:16–8:19). The portion of Houser cited by Petitioner indicates that performing verification processing by another electronic document security application is preferred

because it facilitates communication of electronic documents between users. *Id.* at 60 (citing Ex. 1004, 8:2–8). For the additional limitation recited in claim 16, Petitioner relies on Houser's description that "[t]he electronic security application may be implemented using a standard computer, such as an IBM PC-compatible computer." *Id.* at 67 (quoting Ex. 1004, 8:50–52).

In disputing Petitioner's contention, Patent Owner relies on its interpretation that the claim "requires the formatted data to be returned to a PC, PDA, cell phone or email device" from which the authentication host computer received the data. Prelim. Resp. 51. As explained in Section II.A., on this record, we are not persuaded that received data must be returned to the same place from which it was received.

Thus, based on the record before us, we determine the information in the Petition demonstrates that it is more likely than not that claim 16 is anticipated by Houser.

F. Asserted Ground that Claims 2 and 4 Would Have Been Obvious Over Houser and Yoshiura

Petitioner asserts claims 2 and 4, each of which depends from independent claim 1, would have been obvious over Houser and Yoshiura. Pet. 71–73.

1. Dependent Claim 2

Claim 2 additionally recites "the formatted data is a web page." Yoshiura checks the validity of a web page by checking the validity of a "mark." *See* Ex. 1005, 37:42–45, 37:56–38:1. To do so, a digital signature, which is embedded in the mark displayed on the web page, is validated.

See id. at 37:19–30, 37:49–38:4. If the digital signature is valid, a message is displayed that the mark was validated; but if the digital signature is not valid, a message is displayed that the mark was not validated. *See id.* at 37:56–38:8, Fig. 9 (display unit 1102).

Regarding claim 2, Petitioner relies on Yoshiura's description of checking the validity of a web page by using a digital signature embedded in a "mark" on the web page. Pet. 71. According to Petitioner, Yoshiura's checking the validity discloses authenticating, Yoshiura's digital signature discloses the recited "authenticity key," and Yoshiura's embedded "mark" on a web page discloses the formatted data. *Id.* Petitioner also relies on Yoshiura's description of displaying a message stating that the mark was validated, which according to Petitioner, discloses the recited "authenticity stamp." *Id.* Petitioner contends, with support from its declarant Mr. Schneier, that "[i]t would have been obvious to one of ordinary skill in the art to extend the 'electronic document' authentication process of Houser to also include authenticating web pages, as taught by Yoshiura, . . . to extend the usefulness of Houser's 'electronic security application' to include an increasingly popular form of electronic document, *i.e.*, a web page." *Id.* at 72 (citing Ex. 1008 ¶ 98).

Patent Owner contends that Petitioner failed explain why a person of ordinary skill in the art would have been motivated to apply Yoshiura's teachings to the system of Houser. Prelim. Resp. 59. Contrary to Patent Owner's contention, Petitioner, with support from its declarant, contends that a person of ordinary skill in the art would have combined Houser with

Yoshiura "to extend the usefulness of Houser's 'electronic security application' to include an increasingly popular form of electronic document, *i.e.*, a web page." Pet. 72 (citing Ex. 1008 ¶ 98).

On this record and for purposes of institution, we are satisfied that Petitioner's articulated reasoning is supported by sufficient rational underpinnings. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (an apparent reason to combine known elements in the fashion claimed by the patent at issue should be made explicit).

Moreover, based on the record before us, we are persuaded Petitioner has demonstrated a reasonable likelihood it would prevail in showing that claim 2 would have been obvious over Houser and Yoshiura.

2. Dependent Claim 4

Claim 4 additionally recites "displaying the formatted data in response to the verification of the authenticity key." Regarding claim 4, Petitioner relies on Yoshiura's description that its web page is not displayed until the web page has been authenticated. Pet. 72 (citing Ex. 1005, 29:8–13, 32:11–17).

Patent Owner contends that Petitioner failed explain why a person of ordinary skill in the art would have been motivated to apply Yoshiura's teachings to the system of Houser. Prelim. Resp. 62. Contrary to Patent Owner's contention, Petitioner, with support from its declarant, contends that a person of ordinary skill in the art would have combined Houser with Yoshiura to "facilitate the viewer's ability to detect that the document has not been authenticated." Pet. 73 (citing Ex. 1008 ¶ 100).

On this record and for purposes of institution, we are satisfied that Petitioner's articulated reasoning is supported by sufficient rational underpinnings. *See KSR*, 550 U.S. at 418.

Moreover, based on the record before us, we are persuaded Petitioner has demonstrated a reasonable likelihood it would prevail in showing that claim 4 would have been obvious over Houser and Yoshiura.

III. CONCLUSION

For the foregoing reasons, we determine that the information presented in the Petition would demonstrate that it is more likely than not that at least one of the claims challenged in the Petition is unpatentable. Any discussion of facts in this Decision is made only for the purposes of institution and is not dispositive of any issue related to any ground on which we institute review. The Board has not made a final determination under 35 U.S.C. § 328(a) with respect to the patentability of the challenged claims. Our final determination will be based on the record as fully developed during trial.

IV. ORDER

For the foregoing reasons, it is

ORDERED that pursuant to 35 U.S.C. § 324(a), a covered business method patent review is hereby instituted as to claims 1–5, 16, and 29–32 of the '191 patent on the following grounds:

Claims 1, 3, 5, 16, and 29–32 under 35 U.S.C. § 102 as being anticipated by Houser; and

Claims 2 and 4 under 35 U.S.C. § 103 as being unpatentable over Houser and Yoshiura;

FURTHER ORDERED that, pursuant to 35 U.S.C. § 324(d) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial, the trial commencing on the entry date of this Order; and

FURTHER ORDERED that the trial is limited to the grounds identified above and no other grounds set forth in the Petition are authorized.

For PETITIONER:

Jonathan M. Lindsay
jlindsay@crowell.com

Jeffrey D. Sanok
jsanok@crowell.com

For PATENT OWNER:

Gregory J. Gonsalves
gonsalves@gonsalveslawfirm.com

André J. Bahou
aj.bahou@secureaxcess.com