Trials@uspto.gov
571-272-7822

Paper 10
Entered: September 9, 2014

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PNC BANK, NATIONAL ASSOCIATION, U.S. BANK, NATIONAL ASSOCIATION, and U.S. BANCORP,
Petitioner,

v.

SECURE AXCESS, LLC,
Patent Owner.

Case CBM2014-00100
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

PNC Bank, National Association ("PNC"), U.S. Bank, National Association, and U.S. Bancorp (together, "U.S. Bank; collectively with PNC, "Petitioner") filed a Petition (Paper 3, "Pet.") requesting a review under the transitional program for covered business method patents of U.S. Patent No. 7,631,191 B2 (Ex. 1001, "the '191 patent"). Secure Axcess, LLC ("Patent Owner") filed a Preliminary Response ("Prelim. Resp."). Paper 7. The Board has jurisdiction under 35 U.S.C. § 324.[1]

The standard for instituting a covered business method patent review is set forth in 35 U.S.C. § 324(a), which provides as follows:

> THRESHOLD.—The Director may not authorize a post-grant review to be instituted unless the Director determines that the information presented in the petition filed under section 321, if such information is not rebutted, would demonstrate that it is more likely than not that at least 1 of the claims challenged in the petition is unpatentable.

Petitioner challenges the patentability of claims 1-32 of the '191 patent under 35 U.S.C. §§ 101, 103, and 112. Taking into account Patent Owner's Preliminary Response, we determine the information presented in the Petition demonstrates it is more likely than not that the challenged claims are unpatentable. Accordingly, pursuant to 35 U.S.C. § 324, we authorize a covered business method patent review to be instituted as to claims 1-32 of the '191 patent.

---

[1] *See* Section 18(a) of the Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284, 329 (2011) ("AIA").

A. Related Matters

Petitioner represents that the '191 patent has been asserted against PNC in *Secure Axcess, LLC v. PNC Bank, National Ass'n*, Case No. 6:13-cv-00722-LED (E.D. Tex.) and has been asserted against U.S. Bank in *Secure Axcess, LLC v. U.S. Bank, National Ass'n*, Case No. 6:13-cv-00717-LED (E.D. Tex.). Pet. 2, Paper 6. Petitioner also identifies sixteen other court proceedings in which Patent Owner has asserted the '191 patent. *See* Pet. 2-3; *see also* Paper 6 (Patent Owner's Related Matters).

Petitioner also identifies a request for an *inter partes* review of the '191 patent filed by a different petitioner—*EMC Corp. v. Secure Axcess, LLC*, Case IPR2014–00475 (PTAB), Paper 3. Pet. 3.

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 2:60-62.

Figures 1 and 2 are set forth below:

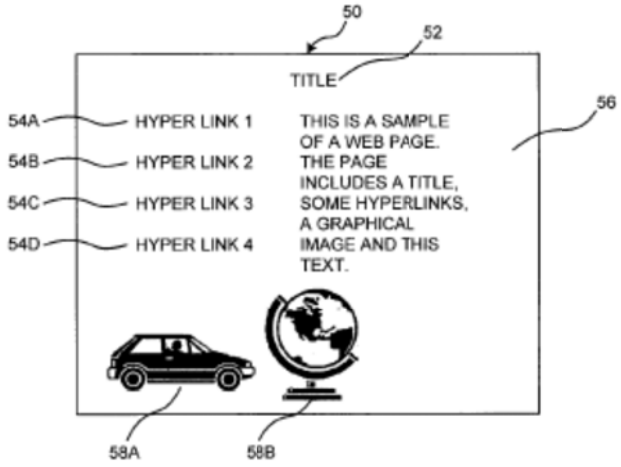

Figure 1

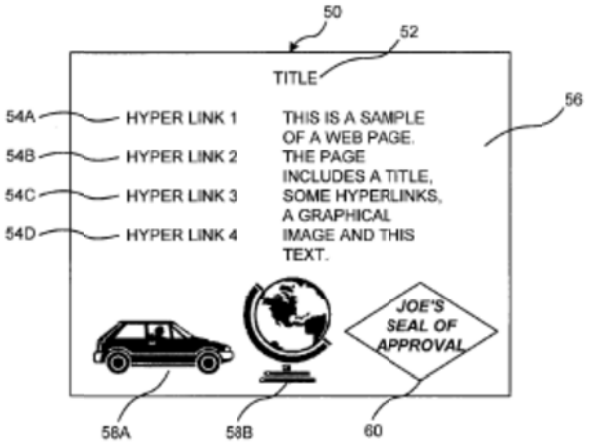

Figure 2

Figures 1 and 2 each show 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 all thirty-two claims of the '191 patent. Claims 1, 17, 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

Petitioner asserts that the challenged claims are unpatentable based on the following grounds:

Basis	Challenged Claims	References
§ 101	1-32	
§ 103	1-32	SHTTP[2] and Arent[3]
§ 103	1-32	SHTTP, Arent, and Palage[4]
§ 112	1-16, 29-32	

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. 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. *Bancorp Servs., L.L.C. v. Sun Life Assurance Co. of Canada*, 687 F.3d 1266, 1273–74 (Fed. Cir. 2012) ("[I]t will ordinarily be desirable—and often necessary—to resolve claim construction disputes prior to a § 101 analysis, for the determination of patent eligibility requires a full understanding of the basic

[2] E. RESCORLA & A. SCHIFFMAN, *The Secure HyperText Transfer Protocol*, the Internet Engineering Task Force (July 1996) (Ex. 1009) ("SHTTP").
[3] U.S. Patent 6,018,724, issued Jan. 25, 2000 (Ex. 1010) ("Arent").
[4] U.S. Patent 6,018,801, issued Jan. 25, 2000 (Ex. 1011) ("Palage").

character of the claimed subject matter."). 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). 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. 15-19; Prelim. Resp. 9-18. For purposes of this decision, we only construe "insert [or "inserting"] an authenticity key" and "received data." We also determine, on this record, whether the recited authenticity key itself is required to locate a preferences file. No other terms in the challenged claims require express construction for this decision.

1. "insert an authenticity key" or "*"inserting an authenticity key"*

Each of independent claims 1, 31, and 32[5] recites "inserting an authenticity key to create formatted data," and independent claim 17 recites "an authentication processor configured to insert an authenticity key into formatted data."

Neither Petitioner nor Patent Owner proposes an express construction for inserting an authenticity key. As made clear by Patent Owner's arguments concerning the asserted prior art, Patent Owner contends the

[5] More precisely, claim 32 recites "inserting an authenticity key to create the formatted data."

recited "inserting" does not encompass "attaching" an authentication key to a document. Prelim. Resp. 38. Rather, according to Patent Owner, "transforming, at an authentication host computer, received data by inserting an authenticity key to create formatted data," as recited in claim 1, requires "inserting the [authentication key] into data received by a host computer." *Id.*

The '191 patent does not set forth a special definition for "insert" or "inserting." Accordingly, we look to the ordinary meaning of the term "insert"— to put or set into, between, or among.[6] The '191 patent describes an authenticity key being inserted into a web page, without further elaboration as: "The logic of FIG. 10 then moves to block 610 where the authenticity key is *inserted* into the web page." Ex. 1001, 8:1-3 (emphasis added); *see also id.* at 1:55-57, Fig. 10 (block 610). The '191 patent's use of "insert" is consistent with its ordinary meaning, which encompasses "being put into."

On this record, we disagree with Patent Owner that "insert" is limited to being put into, and does not encompass being attached to, because Patent Owner has not shown where this term is set forth in the '191 patent in a manner sufficient to supersede the ordinary meaning of the term "insert." If an inventor acts as his or her own lexicographer, the definition must be set forth in the specification with reasonable clarity, deliberateness, and precision. *Renishaw PLC v. Marposs Societa' per Azioni*, 158 F.3d 1243,

[6] AMERICAN HERITAGE DICTIONARY 933 (3d ed. 1992) (defining "insert" as "1. To put or set into, between, or among").

1249 (Fed. Cir. 1998). Patent Owner's construction of "insert" fails to account sufficiently for its ordinary meaning, which is not limited "to put into" but encompasses "to put between or among."

The broadest reasonable construction of "inserting," including inserting by putting among something, encompasses attaching an authentication key to something. Further, the claim language recites "formatted data" (rather than a web page[7]), and so is broader than the embodiment of inserting the authenticity key into the web page. Thus, the claim language is not limited to the embodiment "of inserting into a web page," which appears in the written description. *See In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993); *see also Thorner v. Sony Computer Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012) (It is not enough that the only embodiment, or all of the embodiments, contain a particular limitation to limit a claim to that particular limitation.).

Accordingly, on this record and for purposes of institution, the broadest reasonable construction of "inserting an authenticity key" and "insert an authenticity key" encompasses attaching an authenticity key to the received data to create formatted data.

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

[7] Claim 2, which depends from claim 1, additionally recites "wherein the formatted data is a web page."

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"

One issue raised by Petitioner is whether a preferences file is located by the authenticity key. Petitioner contends that none of the claims require the authenticity key be used to locate the preference file and that the written description only discloses that a preference key, which is different than an authenticity key, is used to locate the preferences file. Pet. 7; *see also* Ex. 1001, 4:38-40 ("Thus, the plug-in 114 must get the preferences key to determine the location of the preferences file."). Petitioner asserts that, if Patent Owner "argues that the authenticity key itself locates a preference file," claims 1-32 would have been obvious over SHTTP, Arent, and Palage. Pet. 71-72.

Patent Owner does not contend that the authenticity key itself locates a preferences file. Rather, Patent Owner proposes the construction of the term "authenticity key" should be "information that (1) indicates that a page should be authenticated and (2) may be used to support authentication." Prelim. Resp. 10; *see id.* at 45. Patent Owner also contends that each of the independent claims only requires "the authenticity key to provide the ability to determine a location of a preference file." Pet. 15. For support, 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. Pet. 16-17 (citing Ex. 1001, 4:37-38, 4:16-25, 9:53-57). According to Patent Owner, an authenticity key enables or provides the ability to determine the location of the preferences file, for example, if determining the location of the preferences file is performed only if the authentication key is verified. Pet. 17.

None of the claims expressly requires that the authenticity key itself locates a preferences file or is used to locate a preferences file. For example, claim 1 recites "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." As such, claim 1 does not require expressly that the authenticity key itself locates a preferences file or is used to locate a preferences file, only that the authenticity key enables locating a preferences file. Similarly to claim 1, independent claim 29 recites "wherein the authenticity key enables location of a preferences file."

Independent claim 17 recites "to insert an authenticity key into formatted data to enable authentication of the authenticity key to verify a

source of the formatted data and to retrieve an authenticity stamp from a preferences file. Although claim 17 recites "to retrieve an authenticity stamp from a preferences file," claim 17 does not recite locating a preferences file, much less reciting that the preferences file is located by an authenticity key.

Independent claims 31 recites "wherein the authenticity key is retrieved from the formatted data to locate a preferences file," and independent clam 32 recites "retrieving, by the client computer, the authenticity key from the formatted data to locate a preferences file." Each of these claims requires retrieving the authenticity key from the formatted data to locate a preferences file. Patent Owner contends, however, these claims only require the authenticity key to provide the ability to determine a location of a preferences file. Pet. 15.

Neither Patent Owner nor Petitioner contends that the authenticity key itself locates a preferences file or is used to locate a preferences file. On this record, we are not persuaded that any claim in the '191 patent requires the authenticity key to locate a preferences file.

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 also* 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. 2, 14; *see also* Paper 6.

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. 18-35; Prelim. Resp. 15-31. "[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 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." AIA § 18(d)(1); *see also* 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 157 Cong. Rec. S5432 (daily ed. Sept. 8, 2011)).

Petitioner contends the ’191 patent meets the financial product or service requirement, because the patent specification includes discussions of financial services using the claimed systems and processes, and because Patent Owner has sued approximately fifty financial institutions, including banks. Pet. 11-12.

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.” Pet. 20; *see also* Pet.18-20. According to Patent Owner, the ’191 patent claims an authentication server that authenticates data (such as a web page) from a service. Pet. 25, 28. As such, Patent Owner contends the ’191 patent is not a covered business method patent, because (1) the claimed method and apparatus can be used by a business generally, and (2) the claim language is devoid of any financial or monetary terms. Pet. 20, 22-25. Patent Owner further contends that asserting the ’191 patent against financial institutions is not sufficient to demonstrate the ’191 patent claims activities that are financial in nature, incidental to a financial activity, or complementary to a financial activity. Prelim. Resp. 26-28.

Based on the record before us, we determine that the method and apparatus claimed by the ’191 patent 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)

and used in commerce, including (i) transacting business over a network, such as the Internet (*id*. at 10:65-11:3); and (ii) selling of goods, services, or information over a network (*id.* at 17-21). 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.

Because the method and apparatus claimed by the '191 patent are incidental to a financial activity, 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 also* 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 claims do not solve a technical problem using a technical solution. Pet. 13-14. More specifically, 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 13. 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.* at 13-14.

Patent Owner disagrees. Prelim. Resp. 28-35. 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 29. Patent Owner further contends the claimed subject matter, as a whole, recites a technological solution — a computer system, including an authentication system, an authentication key, and authentication stamp, that executes a particular series of steps. *Id.* at 30, 31.

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 patent specification indicates that components of the computer system used in the claimed authentication process are known technologies. For example, the written description 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 3:38-44, 10:67-11:3, 11:12-17). The patent 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 patent specification describes using known cryptography techniques for encrypting and decrypting the authenticity key. *See id.* at 6:28-32. Also, the patent 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 (Ex. 1001, 2:67-4), 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 the independent claim and dependent claims 2 and 4 (Prelim. Resp. 30), 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. 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.

We also have considered whether the claimed subject matter solves a technical problem using a technical solution, as contended by Patent Owner, (Prelim. Resp. 29, 34-35), but, because we conclude that the claimed subject matter, as a whole, does not recite a technological feature that is novel and unobvious over the prior art, 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 1-32 Are Unpatentable Under § 101

Petitioner challenges claims 1-32 of the '191 patent as directed to patent-ineligible subject matter under 35 U.S.C. § 101. Pet. 72-77. 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. *See Bilski v. Kappos*, 130 S. Ct. 3218, 3222 (2010).

1. Whether the Claims Are Directed to an Abstract Idea

Petitioner challenges each claim of the '191 patent as failing to recite patentable subject matter under § 101, because the claims fall within the judicially created exception encompassing abstract ideas. Pet. 73-76. 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 they 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." *Id.* (quoting *Mayo*, 132 S. Ct. at 1291, 1297).

In other words, the second step is to "search for an 'inventive concept'—*i.e.*, an element or combination of elements that is 'sufficient to ensure that the patent in practice amounts to significantly more than a patent on the [ineligible concept] itself.'" *Id.* (alteration in original) (quoting *Mayo*, 132 S. Ct. at 1294).

Turning to the Petition, Petitioner, relying on the framework set forth in *Mayo* and followed in *Alice*, asserts that claims 1-32 are unpatentable under § 101, because the claims are drawn to patent-ineligible "abstract ideas, with only insignificant, well-known subject matter added." Pet. 73; *see also* Pet. 73-76. Patent Owner disagrees. Prelim. Resp. 56-65.

In determining whether a method or process claim recites an abstract idea, we must examine the claim as a whole. *Alice*, 134 S. Ct. at 2355 n. 3. 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, enabling a particular type of computer file to be located and from which an authenticity stamp is retrieved. On its face, there is nothing immediately apparent about these physical steps that would indicate the claim is directed to an abstract idea.

Moreover, claim 1, as a whole, is distinguishable from the patent-ineligible abstract concepts found in *Alice* or *Bilski*. *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. *Bilski* involved the concept of hedging risk, which the Court deemed "a method of organizing human activity." *Bilski*, 130 S. Ct. at 3222. Like the concept of hedging risk in *Bilski*, *Alice's* "concept of intermediated

settlement" was held to be "'a fundamental economic practice long prevalent in our system of commerce.'" *Alice*, 134 S. Ct. at 2356. Similarly, the Court in *Alice* found that "[t]he use of a third-party intermediary . . . is also a building block of the modern economy." *Id.* "Thus," the Court held, "intermediated settlement . . . is an 'abstract idea' beyond the scope of § 101." *Id.*

Petitioner asserts that claim 1 is an abstract idea, because it is nothing more than computerizing a purported centuries old practice of placing a trusted stamp or seal on a document to indicate the authenticity of the document. Pet. 74. Petitioner's position is unpersuasive, because as indicated by Patent Owner (Prelim. Resp. 64-65), Petitioner does not tie adequately the claim language to the purported abstract concept of placing a trusted stamp or seal on a document. Although the claim recites retrieving an authenticity stamp, the claim does not recite placing the stamp, much less doing so on a paper document, presumably as "centuries-old" practices have done. Similarly, the claim does not recite a paper document. Moreover, claim 2, which depends from claim 1, additionally recites that the formatted data is a web page, not a paper document.

We also find that Petitioner does not provide sufficient persuasive evidentiary support that the placing of a trusted stamp or seal on a document is "a fundamental economic practice" or a "building block of the modern economy." *See Alice*, 134 S. Ct. at 2356 (citing various references concerning the concept of intermediated settlement, including an 1896 reference).

Petitioner further asserts claim 1 is patent-ineligible abstract idea, because it "relates to nothing more than manipulating and collecting data." Pet. 73 (citing *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1370 (Fed. Cir. 2011); *In re Grams*, 888 F.2d 835, 840 (Fed. Cir. 1989)). Patent Owner disagrees, indicating that claim 1 recites (1) transforming at an authentication host computer, received data (a) by inserting an authenticity key (b) to create formatted data; and (2) returning, from the authentication host computer, the formatted data (a) to enable the authenticity key to be retrieved from the formatted data and (b) to locate a preferences file. Prelim. Resp. 58-59.

Petitioner's reliance on *CyberSource* and *Grams* 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 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 fundamental change to the data; a change that cannot be performed in the human mind.

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. *Grams*, 888 F.3d at 840 (quoting *In re Meyer*, 688 F.2d 789, 794 (CCPA 1982)).

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 does not provide further arguments specifically addressing limitations in claims 2-32 (*see generally* Pet. 73-76).

For these reasons, we are not persuaded by Petitioner's assertion that claims 1-32 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

Petitioner also contends that claims 1-32 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. We understand that the machine-or-transformation test is a useful tool, but is not sole test for whether an

invention is a patent-eligible process under § 101. *See Bilski* 130 S. Ct. at 3227.

Petitioner asserts claim 1 does not transform an article into a different state or thing. Pet. 76. Rather, according to Petitioner, the transforming limitation in claim 1 is merely manipulation or reorganization of data, which is not patent eligible. Pet. 76-77 (citing *CyberSource*, 654 F.3d 1375).

We are not persuaded 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").

Petitioner does not provide persuasive argument or supporting evidence to support its position that the transforming limitation is merely manipulation or reorganization of data. 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 claim 1 does not meet the machine prong of the test. Furthermore, Petitioner does not provide further arguments regarding claims 2-32 (*see generally* Pet. 76-77), thus, we are not persuaded claims 1-32 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 of Obviousness Over SHTTP and Arent

Petitioner asserts that claims 1-32 of the '191 patent are unpatentable under 35 U.S.C. § 103 over SHTTP and Arent.

1. Priority Date of Claims 1-32

Petitioner asserts that Arent, which issued January 25, 2000, is prior art under 35 U.S.C. § 102(a), because Arent issued before the effective filing date of the '191 patent. Pet. 21. Petitioner asserts that September 6, 2000 is the earliest date of which the '191 patent is entitled to claim benefit, because the provisional application (Ex. 1007), of which the '191 patent claims benefit, does not provide the requisite support for any of the claims. Pet. 19-20. Petitioner asserts "[a]t best, the provisional application only generically discloses using a shared secret between a merchant and a consumer for authentication." Pet. 20.

For purposes of this decision, we agree with Petitioner (Pet. 20) that the provisional application does not disclose an authenticity key, as recited in each of independent claims 1, 17, 29, 31, and 32. Accordingly, on this record, we agree with Petitioner that Arent is prior art under 102(a) to the '191 patent.

2. Overview of Asserted Prior Art

SHTTP is a draft document of the Internet Engineering Task Force ("IETF") describing the Secure HyperText Transfer Protocol, which provides secure communication between a client computer and a server to enable commercial transactions. Ex. 1007, 1, 2. SHTTP describes a server attaching a digital signature to a document, which creates a signed document

to be sent to a client computer and used to verify the authenticity of the signed document. *See id.* at 32-33. SHTTP also describes displaying, on the client computer, a visual indicator of the security of the transaction and indicating the identity of the signer of the signed document. *See id.* at 31.

Arent describes authenticating online transaction data. Ex. 1010, Abstract. A validation process is initiated when a user initiates an electronic transaction, and the validation process "determin[es] authenticity of data related to the transaction, such as the identity of a transaction party." *Id.* If the data are authentic, Arent's process displays a "certification indicator," which may be a graphic with user defined text and may be customized by a user. *Id.*

Arent's Figure 4 is set forth below:

FIG. 4

Figure 4 illustrates an example certification indicator. *Id.* at 4:16-17. As shown, certification indicator 400 is displayed on the user's device "as a

graphic that floats above merchant web page 100." *Id.* at 4:17-20. Arent teaches that a user-customized certification indicator stored on the user's device helps protect a user from an unscrupulous merchant counterfeiting a certification indicator. *See id.* at 4:34-50. Arent's Figure 6 is set forth below:

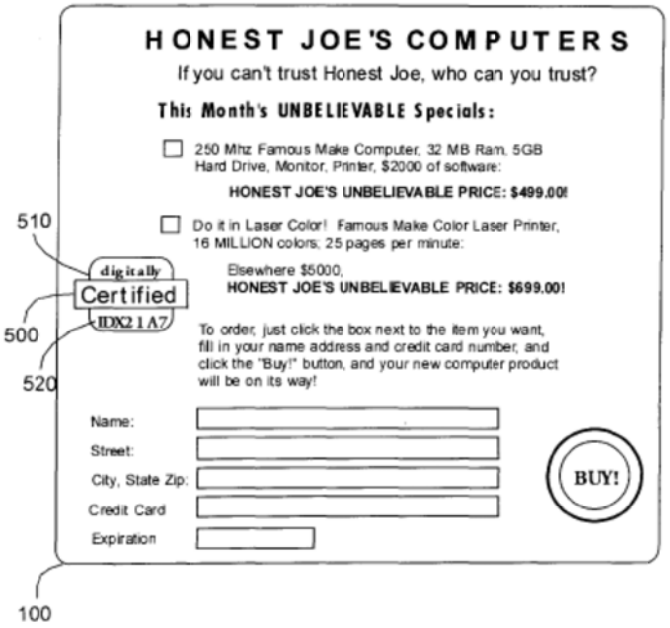

FIG. 6

Figure 6 illustrates an example of certification indicator with a user-defined component. Certification indicator 500 includes standard component 510 and user-defined component 520 consisting of a text string selected by the user and stored in a database with user preference information. *Id.* at 4:51-60, 7:24-25, 7:33-37. After the merchant has been authenticated, components 510 and 520 of the certification indicator are retrieved from storage and combined to form certification indicator 500, which is displayed on top of merchant's web page 100. *Id.* at 4:67-5:7.

3. Analysis

Regarding independent claim 1, Petitioner relies on SHTTP for "teaching 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." Pet. 23.

With respect to claim 1, Petitioner contends the document of SHTTP discloses the recited "received data," SHTTP's server discloses the recited "authentication host computer," and SHTTP's description of the server digitally signing the document discloses the recited "transforming, at an authentication host computer, received data." Pet. 23. Petitioner further contends that SHTTP's digital signature discloses the recited "authenticity key," and SHTTP's signed document discloses the recited "formatted data." *Id.* Petitioner then contends that SHTTP's attaching the digital signature to the document discloses "inserting an authenticity key to create formatted data." *Id.* Petitioner further contends that sending the signed document to a client computer discloses "returning, from the authentication host computer, the formatted data." *Id.*

Petitioner relies on the combination of SHTTP and Arent for disclosing the additional limitations in claim 1—"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." In particular, according to Petitioner, SHTTP describes enabling a client to retrieve the digital signature from the signed document, which discloses retrieving the authenticity key from the formatted data. Pet. 24.

Petitioner relies on Arent as describing one way to implement SHTTP's visual indicator of security. Pet. 21. Petitioner also contends Arent's description that the customization information for the certification indicator is stored in an individual database for a user discloses the recited "preferences file." *Id.* Petitioner relies on SHTTP's digital signature and visual indicator of security in combination with Arent's display of a certification indicator after receiving a digital signature from the merchant as disclosing the recited "to enable the authenticity key to be retrieved from the formatted data and to locate a preferences file." Pet. 26 (citing, e.g., Ex. 1010, 3:38-42).

Petitioner further relies on Arent's certification indicator as disclosing the recited "authenticity stamp" and Arent's database, which stores user-entered components of a certification indicator, as disclosing the recited "preferences file." Pet. 26-27. Petitioner contends Arent's description of retrieving a user-specific text string from the database to form a user-customized certification indicator displayed over a merchant's web page discloses retrieving the authenticity stamp from a preferences file. Pet. 27.

Petitioner contends, with support from its declarant Paul C. Clark (Ex. 1002), "[i]t would have been obvious to a person of ordinary skill in the art at the time of the invention to apply the teachings of *Arent* to implement the visual indicator suggested by" SHTTP. Pet. 22. According to Petitioner, it would have been obvious to combine the references in the proposed manner, because making that combination would be applying known technologies using known techniques and would not yield unexpected or unpredictable results. Pet. 22 (citing Ex. 1002 at 20, ¶ 45). Also, according to Petitioner,

Arent describes advantages of using its customized certification indicator, including preventing unauthorized counterfeiting of the certification indicator. *Id.*

In challenging the Petition, Patent Owner asserts that the combination of SHTTP and Arent does not teach "transforming, at an authentication host computer, received data by inserting an authenticity key to create formatted data," as recited in independent claim 1 or similar limitations recited in independent claims 17, 29, 31, and 32. Prelim. Resp. 37-40. For this limitation, Petitioner relies on SHTTP's description of attaching a digital signature to a document as disclosing inserting an authenticity key to create formatted data, as recited in claim 1. According to Patent Owner, attaching a digital signature is not sufficient to disclose or suggest inserting the digital signature into data received by the host computer. Prelim. Resp. 38. For the reasons stated in section II.A.1, on this record, we determine that the claim language encompasses transforming received data by attaching an authenticity key to the received data to create formatted data. Thus, we are not persuaded by Patent Owner's assertion. Also, we are persuaded, for the reasons stated in section II.A.1 and on this record, that inserting an authenticity key into data required by independent claims 17, 29, 31, and 32 encompasses attaching an authenticity key to received data. *See* Prelim. Resp. 39-40.

Also, regarding the transformation limitation of claim 1 (or similar limitations recited in independent claims 17, 29, 31, and 32), Patent Owner asserts that Petitioner "failed to show that SHTTP teaches that an authentication host computer transforms data that it receives to create

formatted data," because claim 1 "requires an authentication server to receive data sent from elsewhere and transform that data." Prelim. Resp. 38-39. For the reasons stated in section II.A.2, on this record, we are not persuaded that "received data" recited in claim 1 is limited to data that is sent from a device other than the authentication host computer and, thus, does not require receiving data sent from a component in or associated with the authentication host computer.

Second, Patent Owner asserts that SHTTP does not disclose "returning, from the authentication host computer, the formatted data," as recited in claim 1, and similar limitations recited in independent claims 31 and 32. Prelim. Resp. 40-42. According to Patent Owner, the claim limitation "requires the formatted data to be sent by the authentication host computer to the same location from which it received the data," because such a construction is consistent with everyday examples of "returning" to the location from which an item, such as a gift or a purchase, originated. Prelim. Resp. 40-41.

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 and sending a signed document to a client computer does not disclose the returning limitation. Claim 1 does not recite expressly the location to which the formatted data is returned. Furthermore, on this record, Patent Owner fails to demonstrate persuasively 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 (Pet. 42). 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 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. 42.

For these reasons, we are persuaded by Petitioner that the combination of SHTTP and Arent, more likely than not, discloses or suggests the limitations in claim 1. Also, on this record and for purposes of institution, we are satisfied that Petitioner's articulated reason to combine the references to arrive at the claimed invention 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 should be made explicit).

Similarly, having reviewed the Petition, we are persuaded that the combination of SHTTP and Arent proposed by Petitioner, more likely than not, discloses or suggests the limitations in claims 2-32, and we are satisfied,

for purposes of institution and on this record, that Petitioner's articulated reasons to combine the references to arrive at the claimed inventions recited in claims 2-32 are supported by sufficient rational underpinnings. *See generally* Pet. 27-71.

Accordingly, having considered the information in the Petition and Patent Owner's Preliminary Response, we conclude Petitioner has demonstrated it is more likely than not that claims 1-32 would have been obvious over SHTTP and Arent.

E. Asserted Ground of Obviousness Over SHTTP, Arent, and Palage

In the alternative, Petitioner asserts that, if Patent Owner asserts that the authenticity key itself locates a preferences file, claims 1-32 of the '191 patent are unpatentable under 35 U.S.C. § 103 over SHTTP, Arent, and Palage. Pet. 71. Patent Owner proposes the broadest reasonable construction of "to enable the authenticity key . . . to locate a preferences file," as recited in claim 1, requires "the authenticity key to provide the ability to determine a location of a preference file." Prelim. Resp. 15. For the reasons stated in section II.A.3, we are not persuaded that any claim in the '191 patent requires the authenticity key to locate a preferences file.

Accordingly, this alleged ground of unpatentability is redundant to the challenge based on SHTTP and Arent, on which we institute an *inter partes* review. Accordingly, we do not authorize an *inter partes* review on this asserted ground of unpatentability. *See* 37 C.F.R. § 42.208(a); *see also* 35 U.S.C. § 324(a).

F. Asserted Ground that Claims 1-16 and 29-32 Are Unpatentable Under the First Paragraph of § 112

In the alternative, Petitioner asserts that, if Patent Owner asserts that the authenticity key itself locates a preferences file, then claims 1-16 and 29-32 of the '191 patent do not satisfy the written description requirement of 35 U.S.C. § 112, first paragraph. Pet. 77. For the reasons stated in section II.A.3, we are not persuaded that any claim in the '191 patent requires the authenticity key to locate a preferences file. Therefore, we do not institute a review on this asserted ground. *See* 37 C.F.R. § 42.208(a); *see also* 35 U.S.C. § 324(a).

III. CONCLUSION

For the foregoing reasons, we determine that the information presented in the Petition establishes that it is more likely than not that claims 1-32 of the '191 patent are unpatentable. Any discussion of facts in this Decision are made only for the purposes of institution and are 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 1-32 of the '191

patent for the following ground: claims 1-32 under 35 U.S.C. § 103 as being unpatentable over SHTTP and Arent;

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:

Lionel M. Lavenue
Shaobin Zhu
Finnegan, Henderson, Farabow, Garrett & Dunner, LLP
lionel.lavenue@finnegan.com
shaobin.zhu@finnegan.com

For PATENT OWNER:

Gregory Gonsalves
gonsalves@gonsalveslawfirm.com

Andre Bahou
Secure Axcess, LLC
aj.bahou@secureaxcess.com