

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ASKELADDEN L.L.C.,
Petitioner,

v.

XYLON LICENSING, LLC,
Patent Owner.

IPR2021-00658
Patent 8,719,165 B2

Before JOSIAH C. COCKS, ARTHUR M. PESLAK, and
SEAN P. O'HANLON, *Administrative Patent Judges*.

PESLAK, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

Askeladden L.L.C. (“Petitioner”) filed a Petition (Paper 1, “Pet.”) requesting an *inter partes* review of claims 1–8 and 15–18 (the “challenged claims”) of U.S. Patent No. 8,719,165 B2 (Ex. 1001, “the ’165 patent”). Petitioner supports the Petition with the declaration testimony of Ivan Zatkovich. Ex. 1002. We instituted this *inter partes* review as to the challenged claims and all grounds presented in the Petition. Paper 16 (“Dec.”).

During the course of trial, Patent Owner filed a response to the Petition. Paper 19 (“PO Resp.”). Petitioner filed a Reply to the Patent Owner Response. Paper 20 (“Pet. Reply”). Petitioner filed a Supplemental Declaration of Ivan Zatkovich in support of the Petitioner Reply. Ex. 1016. Patent Owner filed a Sur-reply. Paper 26 (“Sur-reply”). An oral hearing was held on June 9, 2022, and a transcript has been entered into the record. Paper 33 (“Tr.”).

We have jurisdiction under 35 U.S.C. § 6. This is a Final Written Decision under 35 U.S.C. § 318(a) as to the patentability of the challenged claims of the ’165 patent. For the reasons discussed below, we determine Petitioner establishes by a preponderance of the evidence that all of the challenged claims are unpatentable.

A. Related Matters

The parties state that the ’165 patent is being asserted or has been asserted in numerous district court litigations. Paper 28; Paper 8. Petitioner is not a party to any of these cases. Paper 28; Paper 8.

The ’165 patent is the subject of an *ex parte* reexamination in Reexamination Control No. 90/014,764. Ex. 1017 (“the reexamination”).

By order entered March 1, 2022, we stayed the reexamination pending completion of this *inter partes* review. Paper 25.

B. Real Parties-In-Interest

Petitioner names itself as the sole Real Party-In-Interest, and states “no other party is in privity with or exercised control or could exercise control over Petitioner’s participation in this proceeding, the filing of this Petition, or the conduct of any ensuing trial.” Pet. 1. Patent Owner names itself as the sole Real Party-In-Interest. Paper 5, 1.

C. The ’165 Patent

The ’165 patent is titled “Delegated Transactions over Mobile.” Ex. 1001, code (54). The ’165 patent generally relates “to enabling completion of secure transactions using mobile devices that may or may not have the needed or desired security features.” *Id.* at code (57). The ’165 patent discloses that a “secure transaction may be partially completed by a secure computing device and partially completed by a less secure mobile device, where the secure computing device may be used to delegate a transaction operation to the less secure mobile device.” *Id.*

Figure 1 of the ’165 patent, reproduced below, is a block diagram of one embodiment of the claimed system, “in which a delegation module 115 is installed on a customer secure computing device 103.” Ex. 1001, 1:29–32.

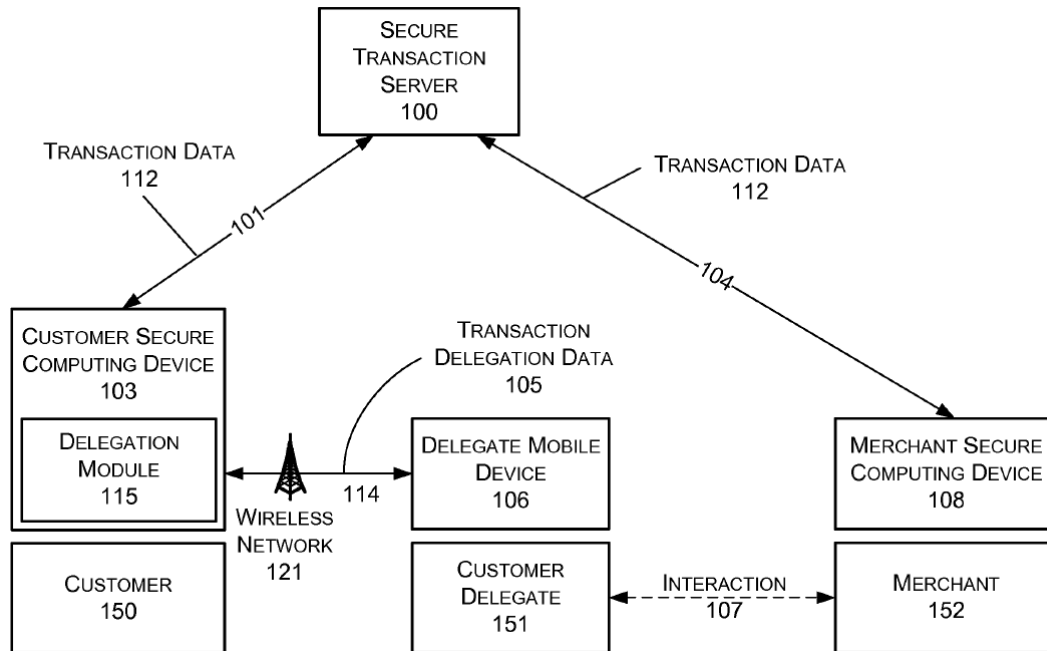


Figure 1 shows customer secure computing device 103, which communicates both with secure transaction server 100 and delegate mobile device 106. *Id.* at 2:35–49.

Figure 2, reproduced below, is a block diagram of another embodiment of the claimed system, “in which a delegation module 125 is installed on a secure transaction server 100.” *Id.* at 1:33–36.

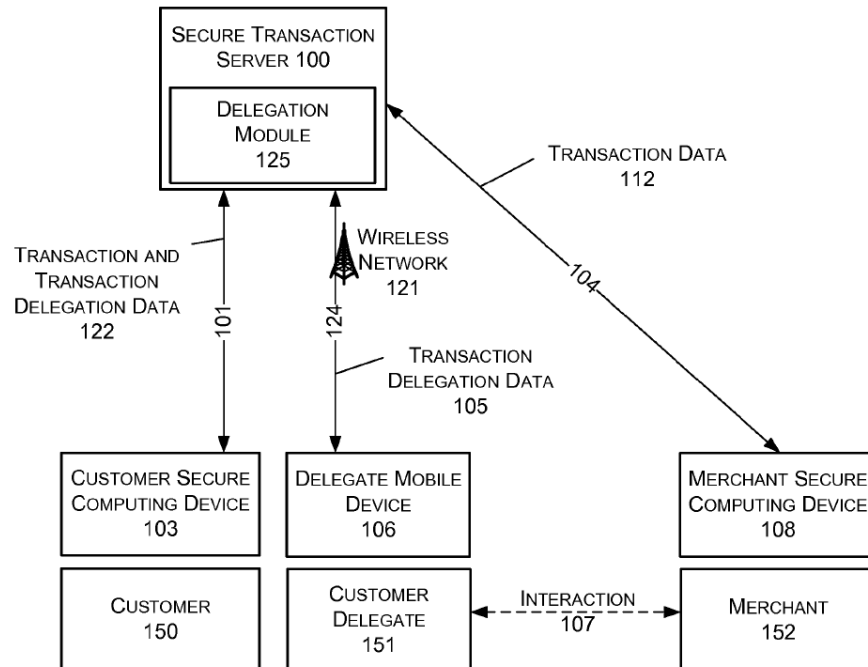


Figure 2 shows secure transaction server 100, which communicates with both customer secure computing device 103 and delegate mobile device 106. *Id.* at 6:43–60.

D. Challenged Claim

Claims 1, 8, and 15 are independent. Claim 1 is illustrative and reproduced below:

1. A method for completing, by a customer secure computing device, a secure transaction between a customer and a merchant, wherein the customer is associated with the customer secure computing device and a delegate mobile device, the method comprising:

acquiring customer delegate mobile device identification information and secure transaction data, by the customer secure computing device, comprising:

receiving, by the customer secure computing device, secure transaction data associated with a delegated transaction, the secure transaction data comprising a merchant identification associated with the merchant;

receiving, by the customer secure computing device, customer delegate mobile device identification information associated with a customer delegate mobile device authorized by the customer for the delegated transaction with the merchant; and
storing, by the customer secure computing device, the secure transaction data and customer delegate mobile device identification information; and
subsequent to acquiring customer delegate mobile device identification information and secure transaction data by the customer secure computing device, automatically completing the secure transaction, by the customer secure computing device, in response to receiving a communication from the identified previously authorized customer delegate mobile device, comprising:
receiving, by the customer secure computing device, a communication from the identified previously authorized customer delegate mobile device;
checking, by the customer secure computing device, a status identifier in the communication from the identified previously authorized customer delegate mobile device; and
automatically initiating, by the customer secure computing device, using the secure transaction data, payment to the merchant by the customer secure computing device in response to receiving the communication from the identified previously authorized customer delegate mobile device, when the status identifier indicates that the delegated transaction is complete.

Ex. 1001, 20:58–21:32.

E. Prior Art and Asserted Grounds

Petitioner asserts that claims 1–8 and 15–18 would have been unpatentable on the following grounds (Pet. 5):

Claim(s) Challenged	Reference(s)	35 U.S.C. §
1–7, 15–18	Wentker ¹	102 and/or 103 ²
8	Drokov ³ , Phillips ⁴	103

II. ANALYSIS

Petitioner bears the burden of establishing the unpatentability of the challenged claims by a preponderance of the evidence. 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d). This burden of persuasion never shifts to Patent Owner. *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

A claim is anticipated under 35 U.S.C. § 102 “only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.” *Verdegaal Bros., Inc. v. Union Oil Co. of Cal.*, 814 F.2d 628, 631 (Fed. Cir. 1987). However, this is not an *ipsissimis verbis* test; i.e., identity of terminology is not required. *See In re Bond*, 910 F.2d 831, 832 (Fed. Cir. 1990).

¹ U.S. Patent Publication No. 2009/0037982 A1, published Feb. 5, 2009 (Ex. 1005) (“Wentker”).

² The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) (“AIA”) included revisions to 35 U.S.C. §§ 102, 103 that became effective on March 16, 2013. Because the ’165 patent was filed prior to March 16, 2013, we apply the pre-AIA versions of 35 U.S.C. §§ 102 and 103.

³ WO 2007/072001A1, published June 28, 2007 (Ex. 1006) (“Drokov”).

⁴ U.S. Patent Publication No. 2009/0166420 A1, published Jul. 2, 2009 (Ex. 1007) (“Phillips”).

A claim is unpatentable under § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) when in evidence, objective indicia of non-obviousness⁵ (i.e., secondary considerations). *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

A. Level of Ordinary Skill in the Art

The level of ordinary skill in the art is “a prism or lens” through which we view the prior art and the claimed invention. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001). The person of ordinary skill in the art is a hypothetical person presumed to have known the relevant art at the time of the invention. *In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995). In determining the level of ordinary skill in the art, we may consider certain factors, including the “type of problems encountered in the art; prior art solutions to those problems; rapidity with which innovations are made; sophistication of the technology; and educational level of active workers in the field.” *Id.*

Petitioner contends that a skilled artisan “would have a bachelor’s degree in computer science, computer engineering, data science, electrical engineering, or a related study and at least one or two years of experience

⁵ Neither party has provided evidence of objective indicia.

with point-of-sale and payment processing systems, credit card transactions, payment settlement and reconciliation, and industry practices and standards for processing of purchase transactions.” Pet. 17 (citing Ex. 1002 ¶¶ 111–113).

Patent Owner does not address the level of ordinary skill in the art. *See generally* PO Resp.

We apply Petitioner’s level of skill in the art because it appears consistent with the problems addressed in the ’165 patent and the prior art.

B. Claim Construction

We apply the same claim construction standard used by Article III federal courts and the International Trade Commission, both of which follow *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc), and its progeny. 37 C.F.R. § 42.100(b) (2020). Accordingly, we construe each challenged claim of the ’165 patent to generally be “the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” *Id.*

Petitioner contends that “the terms of Claims 1-8 [and] 15-18 are clear on their face, except the following claim terms”: “customer secure computing device,” “instruction to enter,” “implements,” and “client.” Pet. 11–17. Patent Owner offers its own construction of “customer secure computing device” and disputes Petitioner’s construction of this term. PO Resp. 5–13.

“customer secure computing device”

Petitioner contends that “customer secure computing device” should be construed as “any ‘device or devices interacting with or on behalf of the customer for processing customer authentication.’” Pet. 13. Petitioner contends the ’165 patent describes examples of the customer secure

computing device as a personal computer or smart phone, but also discloses that “the device could be other types of networked or distributed devices.” *Id.* at 11 (citing Ex. 1001, 3:50–62, 19:5–10; Ex. 1002 ¶¶ 51, 89). Petitioner further contends “the ’165 patent discloses that ‘it is common within the art to describe devices and/or processes in the fashion set forth herein, and thereafter use engineering practices to integrate such described devices and/or processes into data processing systems.’” *Id.* at 11–12 (citing Ex. 1001, 19:19–23; Ex. 1002 ¶¶ 47, 89). Petitioner further contends the ’165 patent “discloses that the architectures of the system described in the ’165 Patent are exemplary and ‘many other architectures may be implemented which achieve the same functionality.’” *Id.* at 12 (citing Ex. 1001, 19:44–46; Ex. 1002 ¶¶ 48, 90).

Petitioner also directs our attention to a construction of “customer secure computing device” by the examiner in the reexamination. Pet. Reply 1. The examiner’s construction is “any device or devices, such as a personal computer, smart phone, or card reader, interacting with or on behalf of the customer for processing customer authentication.” *Id.* (citing Ex. 1017, 18⁶; Ex. 1018, 3–4).

Patent Owner counters with its own construction of “customer secure computing device as “a secure physical device local and proximate to the customer, distinct from the secure transaction server, that the customer uses to initiate or complete a transaction.” PO Resp. 6. In support of this construction, Patent Owner contends “the ’165 Patent clearly defines ‘customer secure computing device’ as physically proximate the user.” *Id.* at 7 (citing Ex. 1001, Fig. 3). Patent Owner directs us to examples in the

⁶ We refer to the page numbers added by Petitioner to Exhibit 1017.

Specification of the '165 patent describing the customer secure computing device as a personal computer or a smart phone. *Id.* at 8 (citing Ex. 1001, 3:50–52, 3:56–62, 6:66–7:1, 8:55–58, 10:58–60). Patent Owner further directs us to portions of the Specification purportedly describing “the customer physically manipulating the ‘customer secure computing device.’” *Id.* at 8–9 (citing Ex. 1001, 1:9–11, 2:23–35, 3:5–8, 3:15–23, 6:65–71, 10:57–60, Fig. 1).

Patent Owner also contends that “Petitioner’s proposed construction of ‘customer secure computing device’ is unduly broad and contrary to the teachings of the specification.” PO Resp. 10. Patent Owner contends that Petitioner’s proposed construction “could arguably encompass the ‘secure transaction server,’ because the secure transaction server ‘interacts’ with a customer.” *Id.* According to Patent Owner, “the specification makes a clear distinction that a secure transaction server is connected over a network connection to the customer secure computing device.” *Id.* at 11 (citing Ex. 1001, 6:53–56, Fig. 3).

Petitioner replies that Patent Owner’s proposed requirement that the customer secure computing device be local and proximate to the customer “is neither explicitly or implicitly required by the specification or the claims.” Pet. Reply 14 (citing Ex. 1016 ¶ 433). According to Petitioner, “that construction would be contrary to the specific teaching of the '165 patent[,] which recognizes that the components may be distributed and therefore not physically proximate to the customer.” *Id.* at 14–15. Petitioner then reiterates its contentions from the Petition “that mechanisms of the invention ‘are capable of being distributed as a program product in a variety of forms.’” *Id.* at 15 (citing Pet. 11–12).

Analysis

We start with the claim language. Claim 1 introduces the term “customer secure computing device” in the preamble of claim 1 and then recites various functions required of the customer secure computing device in subsequent claim limitations. Ex. 1001, 20:58–21:32. We first observe that “secure transaction server” is not recited in claim 1. The language of claim 1, therefore, does not require or suggest any relationship between the customer secure computing device and the secure transaction server requiring that the two be distinct from each other as proposed by Patent Owner. The preamble of claim 1 requires that the customer is “associated with” the customer secure computing device, but nothing in the claim language requires or suggests that the customer secure computing device be local and proximate to the customer.

As noted by both Petitioner and Patent Owner, the Specification of the ’165 patent discloses that the customer secure computing device “may for example comprise a computer device . . . such as for example, a Personal Computer” or it “could also be a secure smart phone.” Ex. 1001, 4:50–57. The Specification also clearly provides that “it will be understood by those within the art that each function and/or operation . . . may be implemented individually and/or collectively, by a wide range of hardware, software, firmware, or virtually any combination thereof.” *Id.* at 18:51–56. This disclosure at column 18 suggests that the customer secure computing device is not limited to the particular examples disclosed in the Specification. In addition, the Specification also discloses that “the subject matter described herein are capable of being distributed as a program product in a variety of

forms.” *Id.* at 19:6–7.⁷ Based on the entirety of the disclosure in the Specification, we determine that the customer secure computing device is not necessarily limited to a physical device local and proximate to the customer. Our determination is in accord with the examiner’s construction of this term in the reexamination, which is not limited to the specifically enumerated physical devices and contains no requirement of proximity to the customer. Ex. 1017, 18.

For these reasons, we determine that Patent Owner’s proposed construction of customer secure computing device is not supported by the evidence before us and do not adopt that construction. Because Petitioner’s proposed construction hews much more closely to the relevant evidence, we apply that construction in our analysis of Petitioner’s challenges.

After reviewing the evidence and argument presented by the parties, we determine that it is not necessary to our decision to construe any other claim terms. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (citing *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) (noting that “we need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy’”).

*C. Alleged Anticipation/Obviousness of
Claims 1–7 and 15–18 over Wentker*

Petitioner asserts that claims 1–7 and 15–18 of the ’165 patent are unpatentable under either 35 U.S.C. § 102(a) and/or § 102(e) and/or § 103(a)

⁷ One of ordinary skill in the art would understand “distributed” in this context to refer to implementing functionality on a remote server in a distributed form in order to service the requests of one or more customer computers.” Ex. 1016 ¶ 435.

based on Wentker. Pet. 5, 17–72. Patent Owner’s arguments revolve primarily around its contention that Wentker does not disclose the recited “customer secure computing device.” PO Resp. 14–26; Tr. 6:10–16.

We begin our analysis with a brief overview of Wentker. We then address the parties’ contentions with respect to the challenged claims.

1. Wentker (Ex. 1005)

Wentker relates to “authenticating the identity of an individual and validating the profile data of the individual (‘a presenter’) who presents himself or herself to another party (‘an acceptor’) as having a certain identity and having certain corresponding profile data.” Ex. 1005 ¶ 7. Wentker discloses “[t]ransactions initiated and conducted from a remote communication device can be riskier than face-to-face transactions, because conventional face-to-face authentication procedures cannot be performed. For example, it is not possible to check a picture on a consumer’s driver’s license when conducting a remote transaction,” and that therefore a method to authenticate an individual during a remote transaction is desirable. *Id.* ¶¶ 3, 4.

Wentker describes initiating remote transactions from a variety of devices including “mobile phones, smartphones, Internet-connected computers or terminals, and personal digital assistants, such as via a client application running on a mobile or stationary device.” *Id.* ¶¶ 28, 29.

Wentker's Figure 1 is reproduced below:

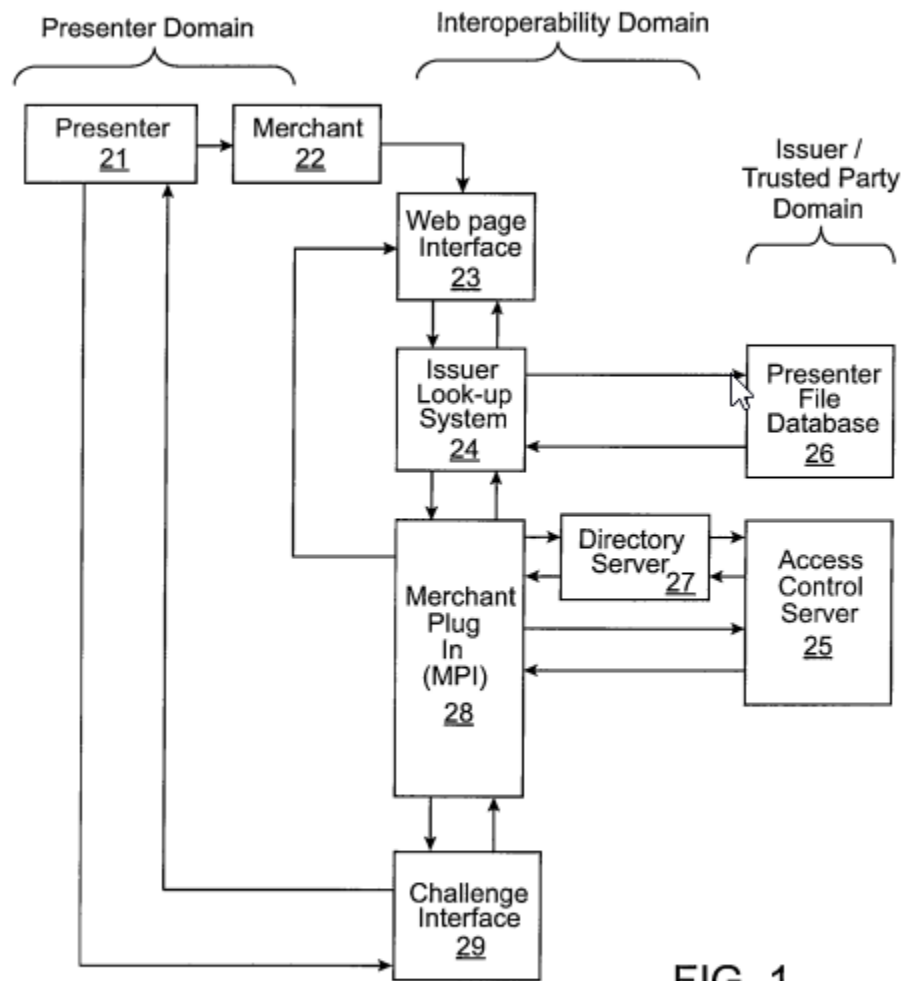


FIG. 1

Figure 1 illustrates “a block diagram of a system according to one embodiment of” Wentker. Ex. 1005 ¶ 13.

Wentker describes that the merchant provides a web page interface 23 “which may be coupled to an issuer look-up system 24,” which in turn “may be operatively coupled to a merchant plug-in (MPI) 28,” and “challenge

interface 29.” Ex. 1005 ¶ 35. Wentker also describes that MPI 28 may be “hosted by an acquirer or other trusted party.” *Id.* ¶ 58. In a transaction, “merchant (MPI) 28 [] issues an authentication challenge to the presenter 21 via the challenge interface 29,” by “send[ing] an authentication challenge to the presenter’s phone.” *Id.* ¶ 59. The customer, “upon receiving the authentication challenge, responds with the predetermined authentication data.” *Id.* ¶ 60.

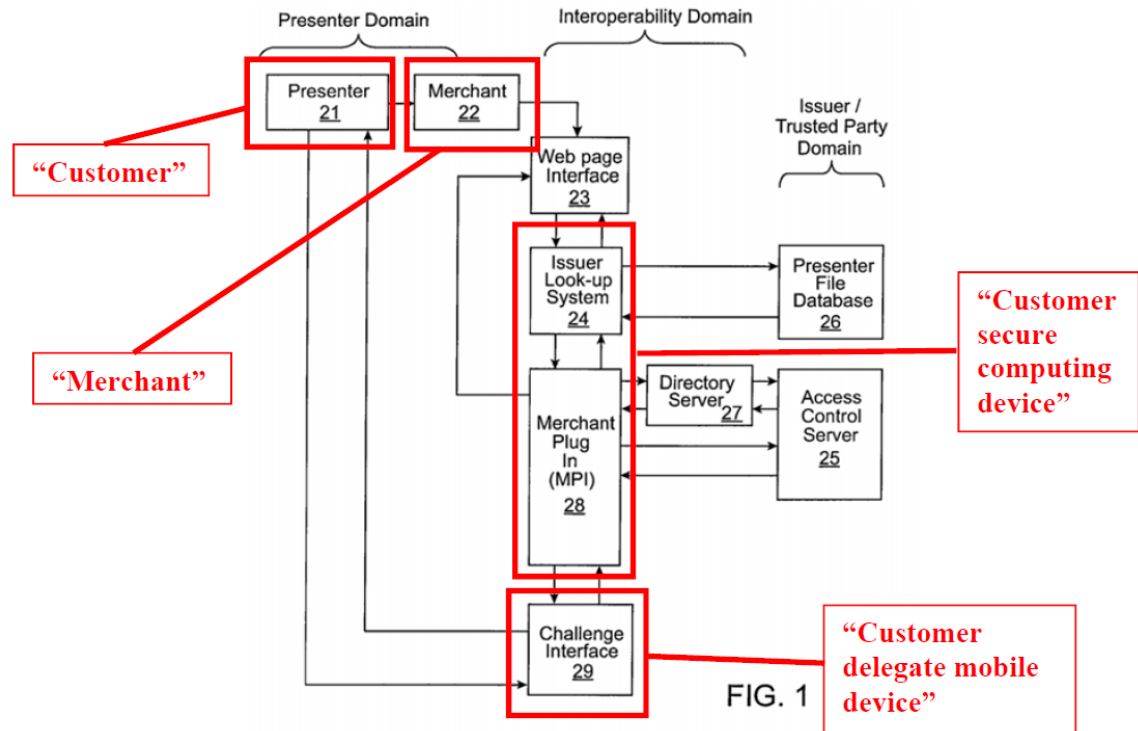
Once the merchant plug-in (MPI) 28 receives the presenter’s authentication data, transaction data (e.g., card data including a card account number and expiration data) are attached and sent to the issuer’s access control server (ACS) 25. The issuer’s access control server (ACS) 25 validates the authentication data and reports the result of the validation to the merchant plug-in (MPI) 28. The merchant plug-in (MPI) 28 then informs the merchant 22 of the result of the verification, for example, through the Web page interface 23.

Id. ¶ 61.

2. *Independent Claim 1*

Petitioner contends that Wentker anticipates or alternatively renders obvious claim 1. Pet. 28–43.

Petitioner provides an annotated version of Wentker’s Figure 1, which is reproduced below.



Petitioner's annotates various items in Wentker's Figure 1 with red rectangles containing text that maps various components of Wentker to elements of the claimed method. Pet. 30. Petitioner contends Wentker's presenter 21 corresponds to the recited customer, merchant 22 corresponds to the recited merchant, issuer look up system 24 and MPI 28 collectively correspond to the recited customer secure computing device, and challenge interface 29 corresponds to the recited customer delegate mobile device. *Id.*

[1PRE]⁸ Preamble: A method for completing, by a customer secure computing device, a secure transaction between a customer and a merchant, wherein the customer is associated with the customer secure computing device and a delegate mobile device, the method comprising:

Petitioner identifies certain elements of Wentker that it contends correspond to the "customer secure computing device" and the "delegate mobile device." Pet. 29. Relying on its proposed construction of "customer

⁸ We use Petitioner's annotations such as [1PRE] for various claim limitations for ease of reference.

secure computing device,” Petitioner contends that Wentker’s “issuer look-up system 24 and the merchant plug-in (MPI) 28 . . . are operatively connected to each other” and “perform each of the steps attributed to the customer secure computing device in Claim 1.” *Id.* (citing Ex. 1002 ¶¶ 155, 156, 161; Ex. 1005 ¶ 35). Petitioner further contends Wentker’s “challenge interface 29” corresponds to the “delegate mobile device . . . which is ‘a client application running on a mobile or stationary device operated by a consumer.’” *Id.* (citing Ex. 1002 ¶ 157; Ex. 1005 ¶¶ 29, 35). Petitioner further contends “Wentker discloses that the customer is associated with the customer secure computing device . . . and a delegate mobile device.” *Id.* (citing Ex. 1002 ¶ 120; Ex. 1005 ¶ 35).

Petitioner contends that the preamble of claim 1 is not limiting. Pet. Reply 4–5. Patent Owner does not address whether the preamble of claim 1 is limiting. *See generally* PO Resp.

Patent Owner, in turn, contends that Wentker’s “issuer look-up system and MPI, operatively coupled” do not meet the requirements of the customer secure computing device as Patent Owner has construed that term. PO Resp. 17–18. Patent Owner argues that these elements in Wentker are not “local and proximate to the customer” and “distinct from the secure transaction server.” *Id.* Patent Owner further contends “the customer never interacts directly with the issuer look-up system or the MPI” and these elements “in Wentker concern[] operations performed on the backend by a merchant server, while the ’165 Patent is directed to this customer secure computing device being used by the customer.” *Id.* at 18. According to Patent Owner, “the ‘customer secure computing device’ needs to be one singular physical device that the customer has locally and proximately, separate from the secure transaction server, which the customer uses to initiate or complete a

transaction.” *Id.*; *see also id.* at 19 (arguing Wentker does not disclose the preamble).

All of Patent Owner’s contentions concerning the customer secure computing device are based on its proposed construction of this term that requires a physical device local and proximate to the customer. Additionally, Patent Owner adds a requirement, not in its proposed construction, that the customer secure computing device “needs to be one singular physical device.” PO Resp. 18. We do not adopt this requirement because it is contrary to the Specification, which states that “the mechanisms of the subject matter described herein are capable of being distributed as a program product in various forms.” Ex. 1001, 19:6–7. Because we do not adopt Patent Owner’s construction, these contentions are all unavailing.

Based on our review of the evidence cited by Petitioner, we find Wentker discloses the subject matter of the preamble and, thus, need not determine whether the preamble is limiting. In particular, Petitioner shows that Wentker’s issuer look-up system 24 and the merchant plug-in (MPI) 28 are devices interacting with or on behalf of the customer for processing customer authentication and which, as explained below, perform the recited operations of the customer secure computing device recited in subsequent limitations.

[1A] acquiring customer delegate mobile device identification information and secure transaction data, by the customer secure computing device, comprising:

Petitioner contends Wentker’s “‘issuer look-up system 24’ portion of the customer secure computing device” performs the acquisition steps, i.e., receives “a merchant identification [][e.g., ‘identity number’]” and “customer delegate mobile device identification information [][e.g., ‘alias identifier.’]”

Pet. 31 (citing Ex. 1002 ¶¶ 162–164; Ex. 1005 ¶¶ 30, 35, 48, 55). Petitioner also contend that Wentker’s alias identifier “can be a ‘phone number.’” *Id.* at 30 (citing Ex. 1005 ¶ 30).

Patent Owner first repeats its contention that Wentker fails to disclose a customer secure computing device based on its construction of this term. PO Resp. 20. This contention is unavailing for the reasons discussed above.

Patent Owner further contends that Wentker’s disclosure of an alias identifier for the customer delegate mobile device fails to satisfy this limitation because, “while the ‘alias identifier’ can be a phone number, Wentker is explicit in teaching that the ‘alias identifier’ is associated with an account” and, according to Patent Owner, the phone number “is tied to an account, and is not used to identify the customer delegate mobile device.” PO Resp. 20 (citing Ex. 1005 ¶ 30).

This claim limitation requires acquiring identification information for the customer delegate mobile device. The ’165 patent provides that such information can be a “telephone number for a delegate mobile device.” Ex. 1001, 4:43–47. Paragraph 30 of Wentker discloses “[t]he alias identifier is associated with an account identifier such (as an account number) for an account of the presenter (e.g., a consumer). The alias identifier can be a phone number and the account identifier can be an account number such as a credit card account number.” Ex. 1005 ¶ 30.

Based on Wentker’s disclosure that the alias identifier can be a phone number, we find that Wentker discloses this claim limitation. The fact that Wentker may or may not tie the phone number to the account is of little import to whether Wentker discloses “acquiring customer delegate mobile device identification information” in the form of a phone number for the mobile device.

[1A.i] receiving, by the customer secure computing device, secure transaction data associated with a delegated transaction, the secure transaction data comprising a merchant identification associated with the merchant;

Petitioner contends that “Wentker discloses receiving, by the ‘issuer look-up system 24’ portion of the customer secure computing device . . . secure transaction data comprising a merchant identification [] e.g., ‘an acceptor identification number’ . . . associated with a delegated transaction.” Pet. 31 (citing Ex. 1002 ¶¶ 165–169; Ex. 1005 ¶¶ 48, 55, Fig. 1). Petitioner alternately contends that it would have been obvious to a skilled artisan “that the issuer look-up system 24 receives an ‘acceptor identification number’ as an ‘identity number’ in order to make sure that the merchant qualifies to process transactions and be paid.” *Id.* at 32 (citing Ex. 1002 ¶ 70).

Patent Owner repeats its contention that Wentker fails to disclose a customer secure computing device based on its construction of this term. PO Resp. 21. This contention is unavailing for the reasons discussed above.

Based on our review of the evidence cited by Petitioner, we find Wentker discloses this limitation and do not reach Petitioner’s alternate contention.

[1.A.ii] receiving, by the customer secure computing device, customer delegate mobile device identification information associated with a customer delegate mobile device authorized by the customer for the delegated transaction with the merchant; and

Petitioner contends that the ’165 patent discloses “that ‘delegate mobile device 106 identification information’ includes a ‘telephone number’ for a delegate mobile device.” Pet. 33 (citing Ex. 1001, 4:43–45; Ex. 1002 ¶ 171). Petitioner further contends that Wentker “receiv[es], by the ‘issuer look-up system 24’ portion of the customer secure computing device, customer delegate mobile device identification information [] e.g., ‘alias

identifier’ that can be a ‘phone number.’” *Id.* (citing Ex. 1002 ¶¶ 85–93, 155, 176–177; Ex. 1005 ¶¶ 30, 35, 55, 67). Petitioner further contends that a skilled artisan “would have understood that at least in embodiments, the issuer look-up system 24 receives an alias identifier, which includes a mobile phone number associated with the presenter’s device.” *Id.* (citing Ex. 1002 ¶ 177). Petitioner alternately contends “it would have been obvious to a [skilled artisan] that the issuer look-up system 24 receives an alias identifier to identify/contact the customer delegate mobile device to send a challenge request.” *Id.*

Patent Owner first repeats its contention that Wentker fails to disclose a customer secure computing device based on its construction of this term. PO Resp. 21–22. This contention is unavailing for the reasons discussed above.

Patent Owner next repeats its contention in connection with limitation 1A that Wentker’s alias identifier does not correspond to the recited customer delegate mobile device identification information. PO Resp. 22. This contention is unavailing for the reasons discussed above.

Based on our review of the evidence cited by Petitioner, we find Wentker discloses this limitation and do not reach Petitioner’s alternate contention.

[1A.iii] storing, by the customer secure computing device, the secure transaction data and customer delegate mobile device identification information; and

Petitioner contends that “Wentker discloses that . . . ‘program identity numbers and account numbers, profile data, and passwords’ are stored in the presenter file database 26.” Pet. 35 (citing Ex. 1002 ¶ 180; Ex. 1005 ¶ 40). Petitioner further contends that a skilled artisan “would have understood that

the issuer look-up system 24 portion of the customer secure computing device . . . performs the step of storing the secure transaction data and customer delegate mobile device identification information in the presenter's file database 26.” *Id.* (citing Ex. 1002 ¶¶ 85–96, 175, 181–182; Ex. 1005 ¶¶ 35, 55). Petitioner alternately contends that it would have been obvious to a skilled artisan “that the issuer look-up system 24 portion of the customer secure computing device stores the transaction data and customer delegate mobile device identification information in the presenter's file database 26 to facilitate performance of the system.” *Id.* (citing Ex. 1002 ¶ 182).

Patent Owner first repeats its contention that Wentker fails to disclose a customer secure computing device based on its construction of this term. PO Resp. 22. This contention is unavailing for the reasons discussed above.

Patent Owner next repeats its contention in connection with limitation 1A that Wentker's alias identifier does not correspond to the recited customer delegate mobile device identification information. PO Resp. 22–23. This contention is unavailing for the reasons discussed above.

Based on our review of the evidence cited by Petitioner, we find Wentker discloses this limitation and do not reach Petitioner's alternate contention.

[1B] subsequent to acquiring customer delegate mobile device identification information and secure transaction data by the customer secure computing device, automatically completing the secure transaction, by the customer secure computing device, in response to receiving a communication from the identified previously authorized customer delegate mobile device

Petitioner contends that Wentker discloses “automatically completing the secure transaction” because “merchant plug-in (MPI) sends a payment authorization request to an authorization system 70 . . . in response to

receiving a communication (e.g., ‘response SMS message including a password’ . . .) from the identified previously authorized customer delegate mobile device.” Pet. 37 (citing Ex. 1002 ¶¶ 85–93, 155, 185; Ex. 1005 ¶¶ 60, 108).

Patent Owner first repeats its contention that Wentker fails to disclose a customer secure computing device based on its construction of this term. PO Resp. 23. This contention is unavailing for the reasons discussed above.

Patent Owner next repeats its contention in connection with limitation 1A that Wentker’s alias identifier does not correspond to the recited customer delegate mobile device identification information. PO Resp. 23. This contention is unavailing for the reasons discussed above.

Based on our review of the evidence cited by Petitioner, we find Wentker discloses this limitation.

[1B.i] receiving, by the customer secure computing device, a communication from the identified previously authorized customer delegate mobile device;

Petitioner contends that a skilled artisan would have understood “that in the context of the payment authentication transaction process of Figure 7, the authentication data is received by MPI 74 from the presenter’s mobile phone during the consumer authentication process.” Pet. 38 (citing Ex. 1002 ¶ 192; Ex. 1005 ¶ 61). Petitioner further contends that Wentker’s Figure 7 discloses “steps 404 and 405 sending the authentication data (e.g. password) from the mobile phone 72 *to the MPI 74*, which is then passed to the access control server 80.” *Id.* (citing Ex. 1002 ¶ 193; Ex. 1005, Fig. 7). Petitioner alternately contends that it would have been obvious to a skilled artisan “that the authentication data is received by the MPI 74 from the presenter’s mobile phone during the consumer authentication process in order to

validate the authentication data and authenticate the consumer before proceeding to the payment authorization.” *Id.* (citing Ex. 1002 ¶ 192).

Patent Owner first repeats its contention that Wentker fails to disclose a customer secure computing device based on its construction of this term. PO Resp. 24. This contention is unavailing for the reasons discussed above.

Patent Owner next repeats its contention in connection with limitation 1A that Wentker’s alias identifier does not correspond to the recited customer delegate mobile device identification information. PO Resp. 24. This contention is unavailing for the reasons discussed above.

Based on our review of the evidence cited by Petitioner, we find Wentker discloses this limitation and do not reach Petitioner’s alternate contention.

[1.B.ii] checking, by the customer secure computing device, a status identifier in the communication from the identified previously authorized customer delegate mobile device; and

Petitioner directs us to step 408 in Figure 7 of Wentker titled “check payer authentication response” and contends this illustrates “checking the authentication data received from the presenter’s mobile phone during the consumer authentication process.” Pet. 40 (citing Ex. 1002 ¶ 198; Ex. 1005, Fig. 7). Petitioner contends that “[o]nce the authentication data is sent (in step 406) from the presenter’s mobile phone to the ACS 80,” a skilled artisan “would have understood that the delegated transaction is complete” and would have found it obvious “to check the authentication response in order to complete the delegated transaction.” *Id.* (citing Ex. 1002 ¶ 197; Ex. 1005 ¶ 104).

Patent Owner first repeats its contention that Wentker fails to disclose a customer secure computing device based on its construction of this term.

PO Resp. 24–25. This contention is unavailing for the reasons discussed above.

Patent Owner next repeats its contention in connection with limitation 1A that Wentker’s alias identifier does not correspond to the recited customer delegate mobile device identification information. PO Resp. 25. This contention is unavailing for the reasons discussed above.

Based on our review of the evidence cited by Petitioner, we find Wentker discloses this limitation.

[1B.iii] automatically initiating, by the customer secure computing device, using the secure transaction data, payment to the merchant by the customer secure computing device in response to receiving the communication from the identified previously authorized customer delegate mobile device, when the status identifier indicates that the delegated transaction is complete.

Petitioner contends that the merchant plug-in (MPI) “sends a payment authorization request to an authorization system 70.” Pet. 41 (citing Ex. 1002 ¶¶ 85–93, 155, 205; Ex. 1005 ¶ 108). Petitioner further contends that “Wentker discloses that ‘a consumer . . . can initiate transactions . . . based on a[n] alias identifier’ which may be an ‘identity number . . . which may include an . . . ‘acceptor identification number.’” *Id.* (citing Ex. 1002 ¶ 200; Ex. 1005 ¶¶ 48, 67, 76). Petitioner further contends that “Wentker further discloses that if the consumer is authenticated for the transaction, the process may proceed to the authorization process.” *Id.* at 42 (citing Ex. 1002 ¶ 203; Ex. 1005 ¶ 105). Petitioner directs us to annotated versions of Wentker’s Figures 7 and 8 in support of its contentions. *Id.* at 42–43.

Patent Owner first repeats its contention that Wentker fails to disclose a customer secure computing device based on its construction of this term. PO Resp. 25. This contention is unavailing for the reasons discussed above.

Patent Owner next repeats its contention in connection with limitation 1A that Wentker’s alias identifier does not correspond to the recited customer delegate mobile device identification information. PO Resp. 26. This contention is unavailing for the reasons discussed above.

Based on our review of the evidence cited by Petitioner, we find Wentker discloses this limitation.

Summary of Claim 1

For all the foregoing reasons, we determine Petitioner establishes by a preponderance of the evidence that Wentker anticipates claim 1. Because we determine that Wentker anticipates claim 1, we do not reach Petitioner’s alternate contention that claim 1 would have been obvious over Wentker.

3. Claim 2

Claim 2 depends from claim 1 and recites “further comprising automatically sending, by the customer secure computing device, a payment confirmation to the merchant in response to successfully initiating payment according to the automatically initiating payment operation. Ex. 1001, 21:33–37.

Petitioner contends “Wentker discloses automatically sending, by the ‘merchant plug in (MPI)’ portion of the customer secure computing device . . . a payment confirmation (e.g., ‘payment accepted notification message’ . . .) to the merchant . . . in response to successfully initiating payment according to the automatically initiating payment operation.” Pet. 44 (citing Ex. 1002 ¶¶ 85–93, 155, 207–216; Ex. 1005 ¶ 35, 38, 109); *see also id.* at 46 (providing annotated Figure 1 illustrating the step of sending payment confirmation to the merchant with a red rectangle surrounding arrow between Merchant Plug In 28 and webpage interface 23).

Patent Owner does not address claim 2. *See generally* PO Resp.

Based on our review of the evidence cited by Petitioner, we determine Petitioner establishes by a preponderance of the evidence that Wentker anticipates claim 2.

4. *Claim 3*

Claim 3 depends from claim 1 and recites “further comprising automatically sending, by the customer secure computing device, a payment confirmation to the identified customer delegate mobile device in response to successfully initiating payment according to the automatically initiating payment operation.” Ex. 1001, 21:38–42.

Petitioner contends “Wentker discloses automatically sending, by the ‘merchant plug-in (MPI)’ portion of the customer secure computing device . . . a payment confirmation [] e.g., ‘payment accepted notification message’ . . . to the identified customer delegate mobile device . . . in response to successfully initiating payment according to the automatically initiating payment operation.” Pet. 47 (citing Ex. 1002 ¶¶ 217–221; Ex. 1005 ¶ 109); *see also id.* at 48 (providing annotated Figure 8 illustrating the step of sending payment confirmation to the customer delegate mobile device with a red rectangle surrounding steps 506 and 507).

Patent Owner does not address claim 3. *See generally* PO Resp.

Based on our review of the evidence cited by Petitioner, we determine Petitioner establishes by a preponderance of the evidence that Wentker anticipates claim 3.

5. *Claim 4*

Claim 4 depends from claim 1 and recites “further comprising sending, by the customer secure computing device, an instruction to enter the delegated transaction to the identified customer delegate mobile device

in response to receiving the delegate mobile device identification information.” Ex. 1001, 21:43–47.

Petitioner contends “Wentker discloses sending, by the ‘merchant plug-in’ portion of the customer secure computing device . . . an instruction to enter . . . the delegated transaction to the identified customer delegate mobile device . . . in response to receiving the delegate mobile device identification information.” Pet. 49–50 (citing Ex. 1002 ¶¶ 94–98, 222–227; Ex. 1005 ¶¶ 30, 59, 60).

Patent Owner does not address claim 4. *See generally* PO Resp.

Based on our review of the evidence cited by Petitioner, we determine Petitioner establishes by a preponderance of the evidence that Wentker anticipates claim 4.

6. *Claim 5*

Claim 5 depends from claim 1 and recites “the secure transaction data further comprising one or more of an authorized payment amount, a provisional customer payment funds source identification, and/or an identification of goods.” Ex. 1001, 21:48–51.

Petitioner contends “Wentker discloses that the secure transaction data further comprises an authorized payment amount . . . a provisional customer payment funds source identification . . . e.g., ‘bank identification number’ . . . and/or an identification of goods.” Pet. 49–50 (citing Ex. 1002 ¶¶ 228–235; Ex. 1005 ¶¶ 29, 52, 63, 67).

Patent Owner does not address claim 5. *See generally* PO Resp.

Based on our review of the evidence cited by Petitioner, we determine Petitioner establishes by a preponderance of the evidence that Wentker anticipates claim 5.

7. *Claim 6*

Claim 6 depends from claim 1 and recites “further comprising receiving by the customer secure computing device, payment amount data from the identified customer delegate mobile device.” Ex. 1001, 21:52–54.

Petitioner contends “Wentker discloses receiving, by ‘merchant plug-in (MPI)’ portion of the customer secure computing device . . . payment amount data from the identified customer delegate mobile device.” Pet. 50 (citing Ex. 1002 ¶¶ 236–241; Ex. 1005 ¶¶ 29, 60, 61, 63).

Patent Owner does not address claim 6. *See generally* PO Resp.

Based on our review of the evidence cited by Petitioner, we determine Petitioner establishes by a preponderance of the evidence that Wentker anticipates claim 6.

8. *Claim 7*

Claim 7 depends from claim 1 and recites “wherein automatically initiating payment to the merchant comprises establishing a communication connection to a secure transaction server, wherein the communication connection is utilized for automatically initiating payment.” Ex. 1001, 2:55–59.

Petitioner contends “Wentker discloses automatically initiating payment to the merchant by establishing a communication connection (e.g., ‘remote transactions can be initiated from devices including . . . Internet-connected computers’) to a secure transaction server (e.g., ‘authorization system 70’). Pet. 50 (citing Ex. 1002 ¶ 245; Ex. 1005 ¶¶ 28, 108).

Petitioner further contends “the communication connection is utilized for automatically initiating payment (e.g., ‘the merchant plug-in (MPI) sends a payment authorization request to an authorization system 70 (step 501).’ *Id.* at 50–51 (citing Ex. 1002 ¶¶ 242–247; Ex. 1005 ¶ 108).

Patent Owner does not address claim 7. *See generally* PO Resp.

Based on our review of the evidence cited by Petitioner, we determine Petitioner establishes by a preponderance of the evidence that Wentker anticipates claim 7.

9. Independent Claim 15

Claim 15 is directed to “non-transitory computer readable storage medium having instructions” with limitations substantially similar to the limitations of claims 1, 3, and 5, except the secure transaction can be completed by either a customer secure computing device or a secure transaction server. Ex. 1001, 23:37–24:36. Petitioner relies on substantially the same contentions and evidence advanced for claims 1, 3, and 5. Pet. 51–68.

Patent Owner relies on its contentions for claim 1. PO Resp. 26–27.

For the reasons discussed above in connection with claims 1, 3, and 5, we determine Petitioner establishes by a preponderance of the evidence that claim 15 is anticipated by Wentker.

10. Claim 16

Claim 16 depends from claim 15 and recites “wherein the non-transitory computer readable medium implements a customer delegation client.” Ex. 1001, 24:37–39.

Petitioner contends “Wentker discloses that the non-transitory computer readable medium implements a customer delegation client (e.g., ‘(USSD) protocol may be used to send an authentication challenge to the customer’s cell phone using a challenge interface module 29.’” Pet. 69 (citing Ex. 1002 ¶¶ 311–318; Ex. 1005 ¶ 59).

Patent Owner does not address claim 16. *See generally* PO Resp.

Based on our review of the evidence cited by Petitioner, we determine Petitioner establishes by a preponderance of the evidence that Wentker anticipates claim 16.

11. Claim 17

Claim 17 depends from claim 15 and recites “wherein the non-transitory computer readable medium implements a merchant delegation client.” Ex. 1001, 24:40–42.

Petitioner contends “Wentker discloses that the non-transitory computer readable medium implements a merchant delegation client.” Pet. 70 (citing Ex. 1002 ¶ 234; Ex. 1005 ¶ 35). Petitioner further contends “the merchant 22 may enter the identity number into the Web page interface 23” and in another embodiment “the presenter 21 could enter the identity number directly into the system via Webpage interface 23.” *Id.* (emphasis omitted) (citing Ex. 1002 ¶ 325; Ex. 1005 ¶ 54). Petitioner further contends “Wentker discloses that as part of the authentication process, ‘[t]he merchant plug-in (MPI) 28 then informs the merchant 22 of the result of the verification, for example, through the Web page interface 23.” *Id.* (alteration in original) (emphasis omitted) (citing Ex. 1002 ¶ 326; Ex. 1005 ¶ 61).

Patent Owner does not address claim 17. *See generally* PO Resp.

Based on our review of the evidence cited by Petitioner, we determine Petitioner establishes by a preponderance of the evidence that Wentker anticipates claim 17.

12. Claim 18

Claim 18 depends from claim 15 and recites “wherein the non-transitory computer readable medium implements a bank delegation server.” Ex. 1001, 24:43–45.

Petitioner contends “Wentker discloses that the data authentication can include ‘the components shown in the interoperability domain . . . and the issuer/trusted party domain.’” Pet. 72 (citing Ex. 1002 ¶ 332; Ex. 1005 ¶ 34). Petitioner further contends Wentker’s “data authentication system can run an authentication program, and can include a trusted party or components operated by a trusted party” and “the trusted party can be a bank, a credit or debit issuing bank, or a credit or debit card service organization.” *Id.* (emphasis omitted) (citing Ex. 1002 ¶ 332; Ex. 1005 ¶ 37).

Patent Owner does not address claim 18. *See generally* PO Resp.

Based on our review of the evidence cited by Petitioner, we determine Petitioner establishes by a preponderance of the evidence that Wentker anticipates claim 18.

D. Alleged Obviousness of Claim 8 over Drokov and Phillips

Petitioner asserts that claim 8 of the ’165 patent is unpatentable under 35 U.S.C. § 103(a) based on Drokov and Phillips. Pet. 5, 72–91. Patent Owner does not provide arguments for the patentability of claim 8. *See generally* PO Resp.; Tr. 6:1–9.

1. Drokov (Ex. 1006)

Drokov is titled “System and Method for Dynamic Multifactor Authentication.” Ex. 1006, code (54). Drokov “relates to a system and method of dynamically authenticating a user of a communications system,” because “[r]apid growth in the areas of online commercial and banking transactions has necessitated the development of various methods of authenticating users of such systems while preventing identity theft.” *Id.* at 1:3–6. Drokov describes “two-factor authentication” systems to

overcome identify theft, using smartcards, biometrics, and token devices that generate pseudo-random codes. *Id.* at 2:1–28.

Figure 1 of Drokov is reproduced below:

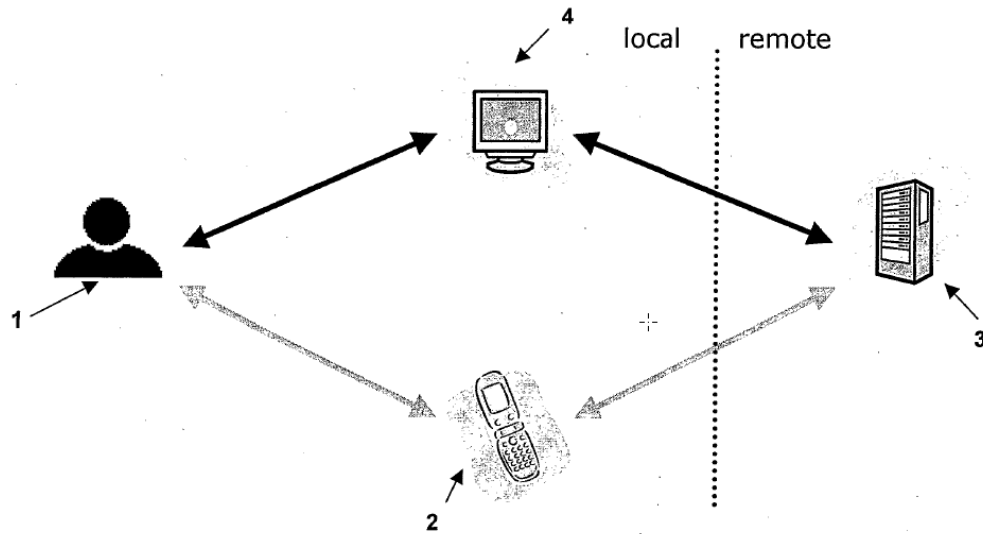


FIGURE 1

Figure 1 is “a diagram representing an authentication system.”

Drokov discloses that, in Figure 1, “a user 1 first makes an authentication request to the remote authentication device 3 via the access terminal 4,” and the “remote authentication device 3 then generates a message which is sent either directly to the mobile device 2 . . . or via any other wireless data communication means.” Ex. 1006, 8:12–23.

Subsequently, “user 1 may then either input the message into the access terminal 4 in order for it to be sent to the remote authentication device 3 or send the message directly to the remote authentication device 3 using the mobile device 2.” *Id.* at 8:24–27.

2. *Phillips (Ex. 1007)*

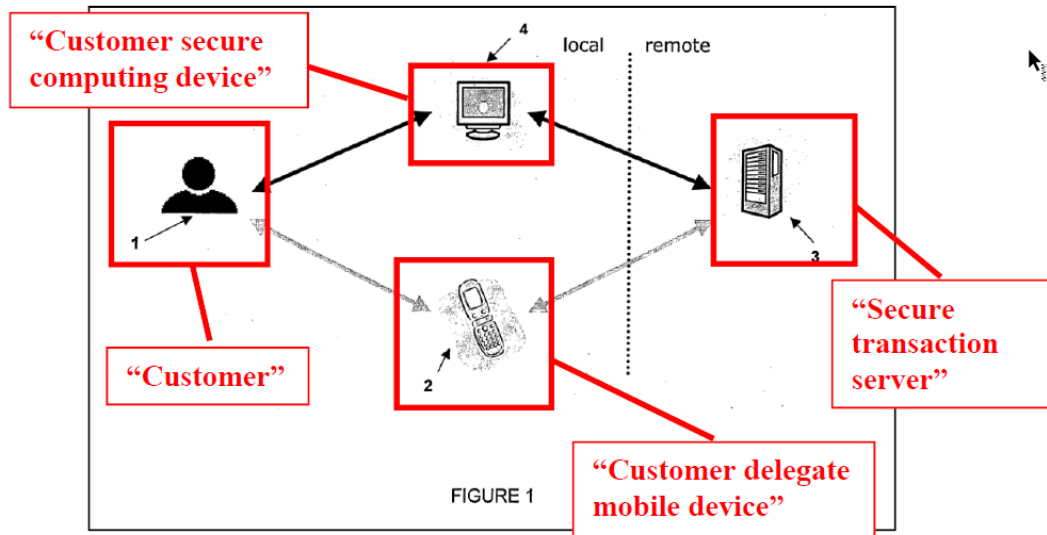
Phillips is titled “Methods and Apparatus for Personalizing Merchant Device for Receiving Contactless Payments.” Ex. 1007, code (54). Phillips describes that “some of the capabilities of a POS terminal/proximity reader be incorporated into a mobile telephone, thereby turning the mobile telephone into a merchant device that is able to receive contactless payments from a contactless payment card or from another mobile device that incorporates contactless payment functionality.” *Id.* ¶ 6. In Phillips, the merchant “device plays the part of the proximity reader, and receives the customer’s payment card account number from the customer’s card or device via wireless communication,” and “then initiates an authorization request for a purchase transaction to an acquirer financial institution that is part of a conventional payment system.” *Id.*

3. *Independent Claim 8*

Petitioner provides contentions with citations to Drokov and Philips (Pet. 78–91) and supports its’ contentions with the testimony of Mr. Zatkovich (Ex. 1002 ¶¶ 334-407). Petitioner contends that “Drokov discloses virtually every element of claim 8.” Pet. 78. Petitioner further contends that “[t]o the extent that Drokov does not explicitly teach” certain claim elements, “Phillips fills the gap such that claim 8 is rendered obvious by Drokov in view of Phillips.” *Id.* at 78–79.

Petitioner also provides reasons why a skilled artisan would have modified Drokov with the teachings of Phillips. Pet. 82–85, 87–88. We reviewed those reasons and, as discussed further below, determine Patent Owner’s contentions to be reasonable and supported by the evidence of record.

Petitioner provides the following annotated version of Drokov's Figure 1 (Pet. 80) with annotations identifying the elements in Drokov that Petitioner contends correspond to the claim elements recited in claim 8:



Petitioner's annotated Figure 1 identifies Drokov's user 1 as corresponding to the "customer," Drokov's access terminal 4 as corresponding to the recited "customer secure computing device," Drokov's mobile device of the user 2 as corresponding to the recited "customer delegate mobile device," and Drokov's remote authentication device 3 as corresponding to the recited "secure transaction server." *Id.* at 79–80.

Preamble: A method for completing, by a secure transaction server, a secure transaction between a customer and a merchant, wherein the customer is associated with a customer secure computing device and a customer delegate mobile device, the method comprising:

Referring to its annotated version of Drokov's Figure 1 reproduced above, Petitioner contends the customer is associated with both "access terminal 4" and a "mobile device." Pet. 79 (citing Ex. 1002, ¶¶ 361–367; Ex. 1006 8:4–11, Abstract). Petitioner further contends that in Drokov, "a user 1 makes an authentication request (associated with a specific transaction the user 1 wishes to perform) to the remote authentication device

3 [secure transaction server] via the access terminal 4.” *Id.* at 80 (citing Ex. 1002 ¶¶ 365–367; Ex. 1006, 8:12–18). Petitioner further contends remote authentication device 3 “replies to the user’s request by sending an authentication code to the user’s mobile device” and then “[t]he user authenticates themselves and confirms the transaction” by entering the authentication code. *Id.*

Based on the evidence cited by Petitioner, we find that Drovok discloses the subject matter of the preamble of claim 8.⁹

[8A] acquiring customer delegate mobile device identification information and secure transaction data, by the secure transaction server, comprising:

Petitioner contends “Drovok discloses acquiring, by the secure transaction server, customer delegate mobile device information (e.g., ‘Subscriber Identify Module (SIM) in the mobile device 2’).” Pet. 80 (citing Ex. 1006, 14:1–2). Petitioner further contends Drovok discloses acquiring secure transaction data (i.e., transactional information) by the secure transaction server and personal information. *Id.* at 80–81 (citing Ex. 1002 ¶¶ 368–369; Ex. 1006 5:25, 9:19, 9:30). Petitioner alternately contends that to the extent Drovok does not explicitly disclose the requirements of this limitation, “Phillips . . . fills the gap such that claim 8 is rendered obvious by Drovok in view of Phillips.” *Id.* at 81 (citing Ex. 1002 ¶¶ 370, 378–380; Ex. 1007).

Based on the evidence cited by Petitioner, we find that Drovok discloses this claim limitation.

⁹ Because we find Drovok discloses the subject matter of the preamble, we need not address whether the preamble is limiting.

[8A.i] receiving by the secure transaction server from the customer secure computing device, secure transaction data and customer delegate mobile device identification information over a secure communication connection with a customer delegation client, wherein the secure transaction data is associated with the merchant, and wherein the customer delegate mobile device identification information is associated with a customer delegate mobile device authorized by the customer for the delegated transaction with the merchant; and

Petitioner contends that Drovok discloses its' remote authentication device receives secure transaction data over a secure communication connection with a customer delegation client because "the message is preferably encoded and encrypted." Pet. 81–82 (citing Ex. 1002 ¶¶ 371, 391; Ex. 1006, 8:19–23). Petitioner further contends that Drovok's secure transaction data is associated with a delegated transaction and comprises a merchant identification associated with the merchant. *Id.* at 82 (citing Ex. 1002 ¶ 370; Ex. 1006, 5:25; 9:19, 9:30, 11:1–3). Petitioner further contends Drovok's customer delegate mobile device identification information is associated with a customer delegate mobile device authorized by the customer for the delegated transaction with the merchant. *Id.* (citing Ex. 1002 ¶ 372; Ex. 1006, 14:1–3).

Petitioner next contends it would have been obvious for a skilled artisan to send a merchant identifier as part of the transactional information to be sent because "the practice was well known and commonly used for merchant credit card transactions." *Id.* at 83 (citing Ex. 1002 ¶ 378; Ex. 1007 ¶ 22). Petitioner further contends it would have been obvious to modify Drovok to include merchant identification information as taught by Phillips and to receive customer delegate mobile device identification information. *Id.* at 84–84 (citing Ex. 1002 ¶¶ 380, 382; Ex. 1006 8:8, 12:26, 14:1–2; Ex. 1007 ¶ 22). Additionally, Petitioner contends a skilled artisan

would have understood that a customer, when entering identifying information in access terminal 4, “would also include other identifying information like the customer’s mobile phone number” because “Drokov needs the customer phone number in order to send and receive authentication messages to/from the customer’s mobile phone.” *Id.* at 84 (citing Ex. 1002 ¶¶ 383–394).

Based on the evidence cited by Petitioner, we find that Drokov in view of Phillips teaches the requirements of this claim limitation.

[8A.ii] storing, by the secure transaction server, the secure transaction data and customer delegate mobile device identification information; and

Petitioner contends Drokov discloses this claim limitation because remote authentication device 3 stores secure transaction data, i.e., “transactional information” and “personal information” such as “account name and password.” Pet. 85 (citing Ex. 1006, 5:25, 8:8, 9:19, 9:30). Petitioner further contends Drokov discloses storing customer delegate mobile device information, i.e., “Subscriber Identity Module (SIM) in the mobile device 2.” *Id.* (citing Ex. 1002 ¶¶ 386–387; Ex. 1006, 14:1–7).

Based on the evidence cited by Petitioner, we find that Drokov discloses this claim limitation.

[8.B] subsequent to acquiring customer delegate mobile device identification information and secure transaction data by the secure transaction server, automatically completing the secure transaction, by the secure transaction server, in response to receiving a communication from the identified previously authorized customer delegate mobile device, comprising:

Petitioner contends Drokov discloses remote authentication server 3 generates an authentication signal in response to receiving a message from the previously authorized customer delegate mobile device. Pet. 88 (citing

Ex. 1002 ¶ 396; Ex. 1006, 8:25, 8:32–9:2). Petitioner further contends that after receiving the message from mobile device 2, remote authentication server 3 checks a status identifier in the message from mobile device 2 and “automatically initiates payment to the merchant if the status identifier indicates that the delegated transaction is complete.” *Id.* at 88–89 (citing Ex. 1002 ¶ 397).

Based on the evidence cited by Petitioner, we find that Drovok discloses this claim limitation.

[8B.i] receiving, by the secure transaction server, a communication from the identified previously authorized customer delegate mobile device

Petitioner contends Drovok discloses “user 1 may . . . send the message directly to the remote authentication device 3 using the mobile device 2.” Pet. 89 (citing Ex. 1002 ¶¶ 398–400; Ex. 1006, 8:8, 8:19–27).

Based on the evidence cited by Petitioner, we find that Drovok discloses this claim limitation.

[8B.ii] checking, by the secure transaction server, a status identifier in the communication from the identified previously authorized customer delegate mobile device; and

Petitioner contends that, in Drovok, mobile device 2 includes a code in the communication to remote authentication server 3 which then “compare[s] the code to the code originally generated” and “[i]f the code matches the code which was originally generated, the user 1 is successfully authenticated.” Pet. 89–90 (citing Ex. 1002 ¶¶ 401–403; Ex. 1006, 8:8, 10:30–35) (emphasis omitted).

Based on the evidence cited by Petitioner, we find that Drovok discloses this claim limitation.

[8B.iii] automatically initiating, by the secure transaction server, using the secure transaction data, a payment to the merchant in response to receiving the communication from the identified previously authorized customer delegate mobile device, when the status identifier indicates that the delegated transaction is complete.

Petitioner contends that a skilled artisan “would have understood that when the server receives the correct code from the mobile device 2, the status of the delegated transaction would be complete, and . . . the server can automatically initiate payment to the merchant by ‘sending an authentication signal.’” Pet. 90–91 (citing Ex. 1002 ¶ 407; Ex. 1006, 5:25, 8:8, 8:26, 9:19, 9:30, 10:30–35, 11:1–3).

Based on the evidence cited by Petitioner, we find that Drovok discloses the requirements of this claim limitation.

Summary of Claim 8

For all the foregoing reasons, we determine that Petitioner establishes by a preponderance of the evidence that claim 8 would have been unpatentable over Drovok and Phillips.

III. CONCLUSION

Weighing the evidence, we determine that Petitioner establishes by a preponderance that claims 1–8 and 15–18 of the ’165 patent are unpatentable.¹⁰

In summary:

¹⁰ Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner’s attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. See 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application

Claims	35 U.S.C. §	Reference(s)/Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1–7, 15–18	102	Wentker	1–7, 15–18	
8	103	Drokov, Phillips	8	
Overall Outcome			1–8, 15–18	

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–8 and 15–18 of the '165 patent have been shown to be unpatentable; and

FURTHER ORDERED that any party seeking judicial review must comply with the notice and service requirements of 37 C.F.R. § 90.2.

or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. *See* 37 C.F.R. §§ 42.8(a)(3), (b)(2).

IPR2021-00658
Patent 8,719,165 B2

For PETITIONER:

Charles Macedo
Keith J. Barkaus
AMSTER, ROTHSTEIN & EBENSTEIN LLP
cmacedo@arelaw.com
kbarkaus@arelaw.com

For PATENT OWNER:

Sanjay Pant
PRA Law
spant@pralawllc.com

Gautham Bodepudi
gbodepudi@outlook.com