

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD.,
Petitioner,

v.

BLAZE MOBILE, INC. and MICHELLE FISHER,
Patent Owner.

IPR2021-01571
Patent 9,378,493 B2

Before HYUN J. JUNG, MIRIAM L. QUINN, and SEAN P. O'HANLON,
Administrative Patent Judges.

QUINN, *Administrative Patent Judge.*

DECISION

Denying Institution of *Inter Partes* Review
35 U.S.C. § 314, 37 C.F.R. § 42.4, 37 C.F.R. § 42.108

I. INTRODUCTION

Samsung Electronics Co., Ltd. (“Petitioner”) filed a Petition (Paper 1, “Petition” or “Pet.”) requesting an *inter partes* review of claims 1–16 (“the challenged claims”) of U.S. Patent No. 9,378,493 B2 (Ex. 1001, “the ’493 patent”) pursuant to 35 U.S.C. §§ 311–319. Blaze Mobile, Inc. and Michelle Fisher (“Patent Owner”)¹ filed a Preliminary Response. Paper 8 (“Preliminary Response” or “Prelim. Resp.”). With our authorization (see Paper 10), Petitioner filed a Preliminary Reply to the Preliminary Response (Paper 11, “Reply”), and Patent Owner filed a Preliminary Sur-reply to the Preliminary Reply (Paper 14, “Sur-reply”).

The standard for institution is set forth in 35 U.S.C. § 314, which provides that an *inter partes* review may not be instituted unless the information presented in the Petition and the Preliminary Response shows that “there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314 (2018); *see also* 37 C.F.R. § 42.4(a) (“The Board institutes the trial on behalf of the Director.”). Upon consideration of the parties’ contentions and the evidence of record, we conclude that Petitioner has not established a reasonable likelihood of prevailing in demonstrating the unpatentability of at least one challenged claim of the ’493 patent. Accordingly, we deny Petitioner’s request and do not institute an *inter partes* review.

¹ Although the parties identify Michelle Fisher as a Patent Owner, Patent Office records indicate Ms. Fisher assigned her interest in the ’493 patent to Blaze Mobile, Inc. with an assignment filed July 24, 2020 at Reel/Frame 053299/0556.

A. Related Matters

The parties identify the declaratory judgment action *Samsung Elec. Co. v. Blaze Mobile Inc.*, Case No. 21-cv-02989-EJD (N.D. Cal.) as a related matter. Pet 2; Paper 12, 1. Petitioner states that the complaint for the declaratory judgment action seeks a judgment of non-infringement for the '493 patent and U.S. Patent No. 9,652,771 ("the '771 patent"). Pet. 2.

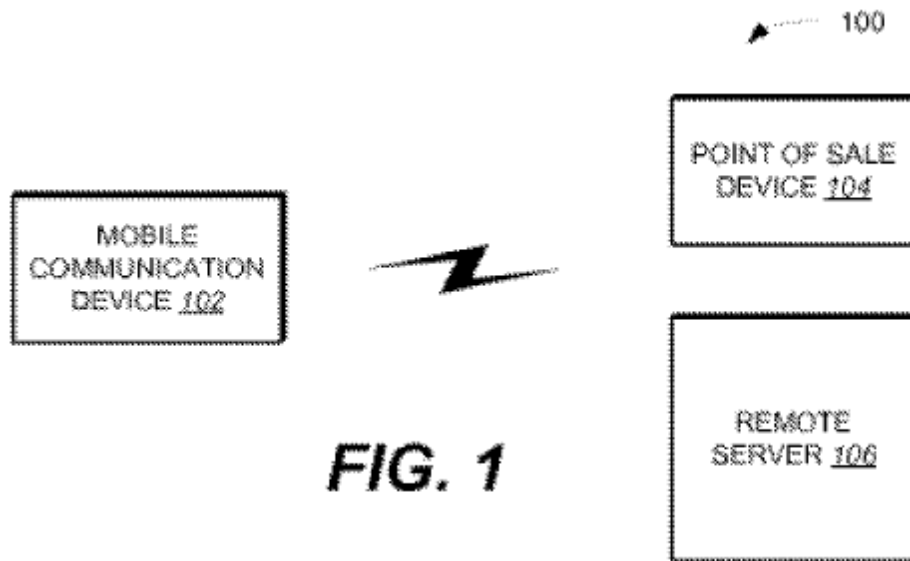
Patent Owner also identifies IPR2021-01569 and IPR2021-01570 as related matters. Paper 12, 1. IPR2021-01569 challenges claims of the '771 patent and IPR2021-01570 challenges claims of U.S. Patent No. 10,565,575. IPR2021-01569, Paper 1, 1; IPR2021-01570, Paper 1, 1. In addition, Patent Owner identifies Application No. 17/363,973 as a related matter. Paper 12, 1–2.

B. The '493 Patent

The '493 patent "relates to data communications and wireless devices." Ex. 1001, 1:16–17. The '493 patent describes mobile communication devices, such as cellular phones, as increasingly being used for payment transactions. *Id.* at 1:21–23. The '493 patent explains that payment transactions can include "purchasing goods and/or services, bill payments, and transferring funds between bank accounts." *Id.* at 1:31–33.

The '493 patent describes "a method for transmitting data between a mobile communication device and a server" that includes running a mobile application on the mobile communication device and transmitting data associated with the mobile application between the mobile communication device and a server that hosts the mobile application. *Id.* at 1:42–50. The '493 patent states that the server monitors the transmission of data between the mobile communication device and the server. *Id.* at 1:50–52.

Figure 1 depicts a block diagram of an implementation of a communication system. *Id.* at 2:18–20.



The '493 patent describes communication system 100 as including handheld, wireless mobile communication device 102, point-of-sale device 104, and remote server 106. *Id.* at 2:33–36. Mobile communication device 102 includes a mobile application that permits a user to conduct payment transactions. *Id.* at 2:36–40.

The mobile application running on the mobile communication device implements tools to secure data that may be stored and presented on the device as a result of a payment transaction. *Id.* at 2:50–54. One such implementation, according to the '493 patent, is to implement security codes for different payment methods to protect the user. *Id.* at 3:4–6. In another implementation, “sensitive information (e.g., banking account numbers, credit card account numbers, expiry dates, and so on) are never stored on the mobile communication device.” *Id.* at 3:31–36.

Further, the '493 patent explains that, in general, some effort is made to minimize the storage of sensitive user information and data on a mobile

communication device. *Id.* at 3:38–40. However, the ’493 patent describes an implementation in which some data is stored in the memory of a mobile communication device for reasons of performance, usability, and user experience. *Id.* at 3:40–42. Thus, the ’493 patent explains that, in one implementation, “a user may opt-in to save payment method security codes in the client (or mobile application) for convenience.” *Id.* at 3:48–50.

C. Illustrative Claims

Of the challenged claims, claims 1 and 9 are independent. Each of challenged claims 2–8 and 10–16 depends directly or indirectly from claims 1 or 9.

Claim 1 is illustrative:

1. A method for conducting a Near Field Communications (NFC) transaction using an NEC protocol and a mobile communication device, the method comprising:

maintaining a secure element application configured to use the NFC protocol and an identification code in a secure element memory in a secure element, the secure element, associated with a mobile communication device comprising of a mobile device memory, a mobile device processor, and a mobile device transceiver, the secure element including the secure element memory, a secure element processor and a secure element communication transceiver supporting a communication channel comprising the (NFC) protocol;

executing the secure element application, wherein the secure element application is executed by the secure element processor in response to detection of a near field communication inductive signal by an NFC terminal, and execution of the secure element application facilitates transfer of the identification code to the NFC terminal using the NFC protocol and further wherein the NFC terminal transfers the identification code to a management server which transmits the identification code to a transaction server for processing of the NFC transaction using a

payment method corresponding to the identification code,
wherein the NFC terminal is configured to use the NFC protocol.

Ex. 1001, 5:46–6:4.

D. Asserted Prior Art and Grounds of Unpatentability

The asserted grounds in this proceeding involve the following prior art references:

a) *Huomo*: WO 2006/095212 A1, published September 14, 2006, filed as Exhibit 1005;

b) *Sklovsky*: US 2008/0162312 A1, published July 3, 2008, filed as Exhibit 1006; and

c) *Dua*: US 8,700,729 B2, issued April 15, 2014, filed as Exhibit 1008.

Petitioner asserts the following grounds of unpatentability (Pet. 5):

Claims Challenged	35 U.S.C. §	References
1–16	103	Huomo, Dua
1–16	103	Sklovsky, Dua

Pet. 5. Petitioner also relies on a Declaration of Dr. Sandeep Chatterjee, filed as Exhibit 1003 (“Chatterjee Declaration” or “Chatterjee Decl.”). Patent Owner relies on an affidavit by Michelle Fisher, filed as Exhibit 2007.

II. ANALYSIS

A. Level of Ordinary Skill in the Art

Petitioner contends that “a person of ordinary skill in the art (‘POSITA’) at the time of the alleged invention would have had a B.S. in Computer Engineering or a related field, or equivalent experience, and two or more years of industry or research experience in data communications, wireless devices, and/or mobile payment systems” and that “[a]dditional education might compensate for less experience, and vice-versa.” Pet. 11

(citing Ex. 1003 ¶ 34). Patent Owner asserts “that a POSITA in the timeframe of the invention would have a bachelor’s degree in computer engineering or similar discipline and approximately two years of experience designing mobile applications for wireless devices.” Prelim. Resp. 7–8.

At this juncture, we do not find it necessary to define the level of skill with specificity save to note that the level of ordinary skill is evidenced by the prior art of record. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001) (stating that the absence of specific findings on the level of skill in the art does not give rise to reversible error where the prior art itself reflects an appropriate level and a need for testimony is not shown).

B. Claim Construction

In *inter partes* review proceedings based on petitions filed on or after November 13, 2018, such as this one, we construe claims using the same claim construction standard that would be used in a civil action under 35 U.S.C. § 282(b), as articulated in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc), and its progeny. *See* 37 C.F.R. § 42.100(b).

The parties appear to dispute the scope of the term “identification code,” and we address this issue below in connection with our determination that Petitioner’s challenge of unpatentability is not sufficiently supported on the present record. Pet. 11; *see generally* Prelim. Resp. Based on the record before us, we determine that no express construction of any term is appropriate.

D. Obviousness Grounds Analysis

Petitioner asserts two grounds of obviousness that we address together below because a single dispositive issue affects both grounds equally. But first, we summarize the prior art asserted, which we discuss in further detail below.

1. *Huomo*

Huomo “relates to the field of control of mobile terminal devices which are equipped with smartcard and near field communications means.” Ex. 1005, 1:7–8. More specifically, Huomo “addresses the field of local communication technology, such as those short-range communications technologies involving electromagnetic/electrostatic coupling technologies and optical short-range communication technologies, namely near field communication technologies (NFC).” *Id.* at 1:9–12.

Huomo describes a method for controlling a mobile terminal device that includes a smartcard module and a near field communication module. *Id.* at 4:12–14. Figure 2a illustrates a schematic arrangement of a smartcard module and is reproduced below.

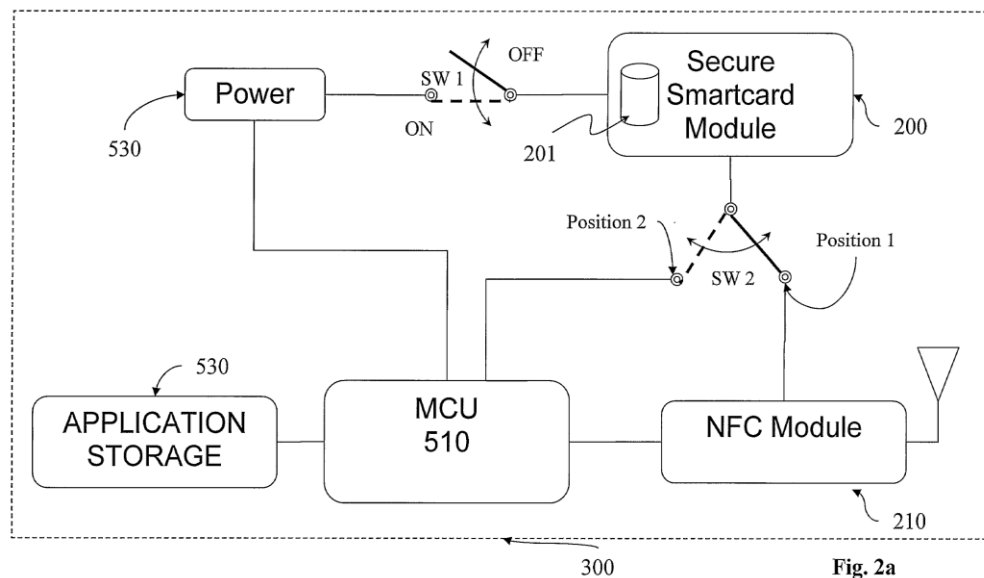


Figure 2a shows an exemplary schematic of a smartcard module and NFC module, as well as other elements, of a mobile device. *Id.* at 12:29–31. Smart card element 200 is integrated into a mobile device and includes secure storage area module 201. *Id.* at 13:1–5. Huomo explains that “secure

storage module 201 may be used for storing different data in a tamperproof environment on the smartcard.” *Id.* at 13:5–6.

Huomo explains that “[a]uthorization is typically done by requesting a certain PIN code from the terminal user in order to activate the secure smart card element 200.” *Id.* at 14:23–24. For instance, an authorization PIN is requested when a user selects a mobile payment application in a terminal’s user interface and, if the PIN is entered correctly, secure smart card element 200 is activated, which in turn activates mobile payment applications. *Id.* at 14:24–27. When a user and transaction provider have mutually agreed to a payment amount, the user “touches” a point-of-sale (POS) terminal NFC interface with the user’s mobile terminal, “so that the necessary information for conducting the agreed transaction will be exchanged.” *Id.* at 17:26–18:1. One such exchange includes mobile terminal 100 providing “credit card information, for instance, including necessary information for conducting the payment for the amount provided by the POS terminal 310.” *Id.* at 18:15–17.

2. Sklovsky

Sklovsky “relates to mobile devices, and more particularly, to contactless transactions using a mobile device.” Ex. 1006 ¶ 2. Sklovsky describes an embodiment in which a system can include an NFC modem for communicating transaction events with an NFC reader, a secure controller for monitoring secure applet events associated with the transaction events, and a mobile host that is communicatively coupled to the secure controller for receiving event notifications via an Applications Programming Interface. *Id.* ¶ 11.

Figure 4 shows a diagram of a secure controller and is reproduced below.

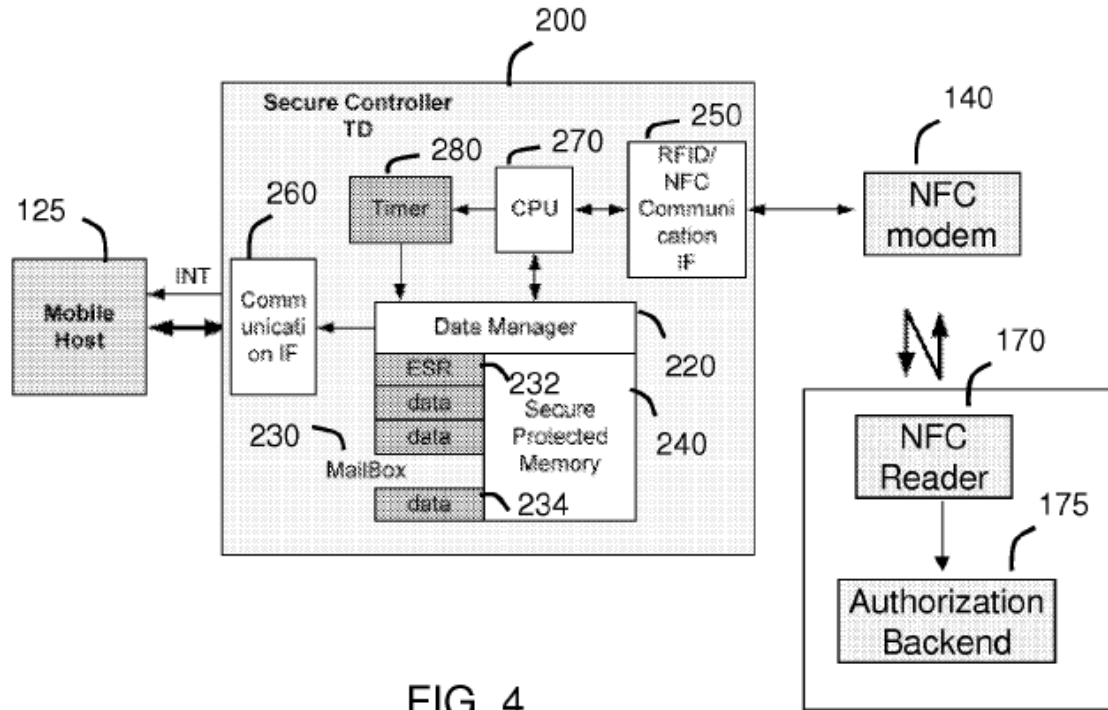


FIG. 4

Figure 4 depicts a block diagram of a secure controller for an NFC/RFID contactless transaction system. *Id.* ¶ 43. Secure controller 200 can include RFID/NFC communication interface 250 to NFC modem 140 for sending and receiving transaction events. *Id.* Data manager 220 is operatively coupled to RFID/NFC communication interface 250 for handling event notifications, and communication interface (CIF) 260 is operatively coupled to mobile host 125 for sending messages to mobile host 125 regarding event notifications. *Id.*

Sklovsky describes mobile host 125 as able to run contactless applications, and secure controller 200 can inform application on mobile host 125 of events or status during secure contactless transactions. *Id.* ¶ 38. For instance, Sklovsky explains that NFC modem 140 may communicate transaction events of a secure contactless transaction with NFC reader 170. *Id.* ¶ 35. According to Sklovsky, “transactions can include the exchange of credit card information, account information, or any other information

associated with the transaction for making a payment.” *Id.* ¶ 63. Sklovsky further explains that data manager 220 can include secure protected memory 240 for storing data and transaction events between NFC modem and NFC reader 170. *Id.* ¶ 44.

3. *Dua*

Dua “relates generally to systems and methodologies for conducting electronic commerce and more particularly to systems and methodologies for issuing, managing, storing and using credentials authorizing the legitimate holder of such a credential to accomplish a desired result.” Ex. 1008, 1:8–12. Dua describes the use of short-range communication network standards by mobile devices to establish wireless connectivity, such as the use of Near Field Communication technology to transfer information to a reader device. *Id.* at 3:13–26.

Dua’s Figure 8 depicts a diagram of an over-the-air PIN verification scheme, which is reproduced below.

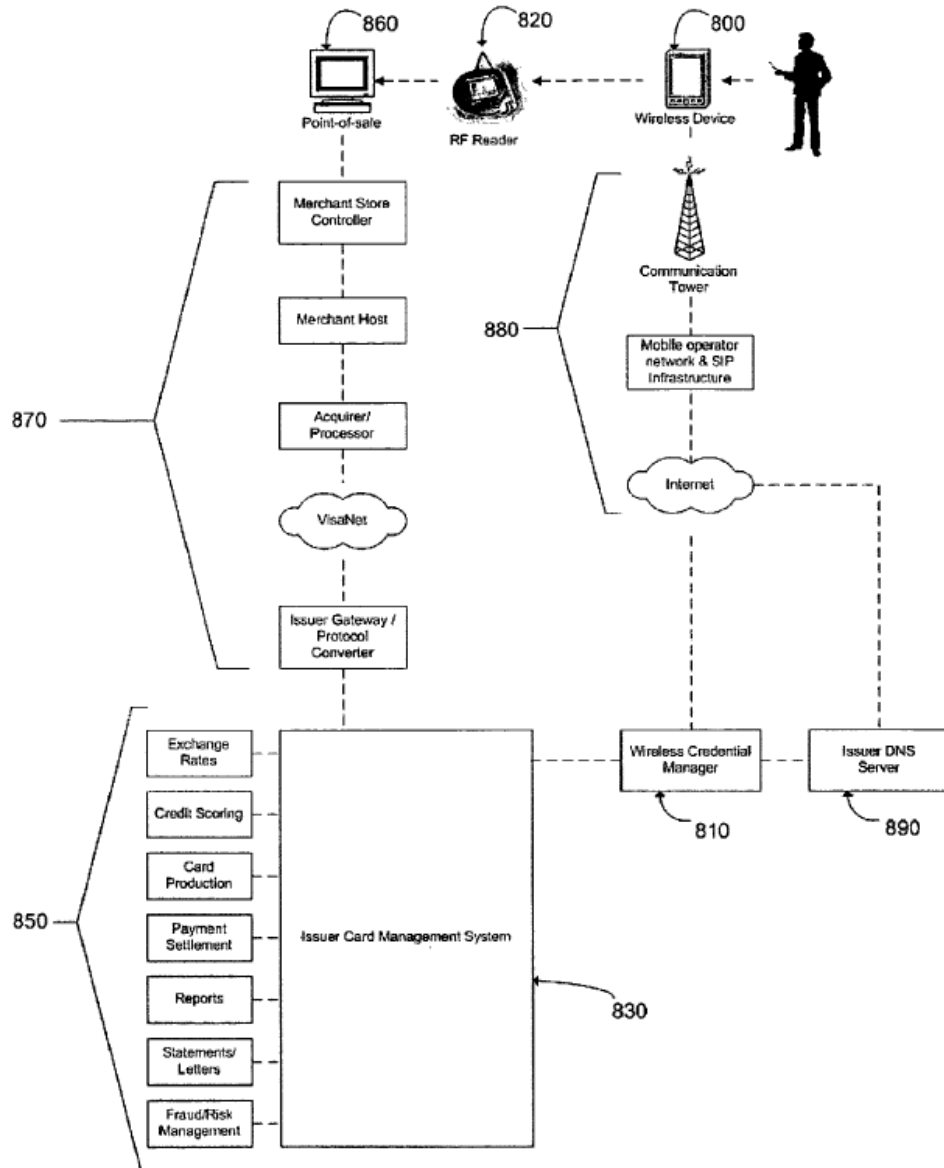


FIG. 8

Dua explains that “a first transmission path of an electronic credit card authorization request S70 includes, for example, a merchant store controller and merchant host system, an acquirer/processor network, a private network such as VisaNet, and a[n] issuer gateway.” *Id.* at 43:53–57. Dua describes point of sale terminal 860 capturing and transmitting an electronic credential from a wireless device via RF reader for online authorization. *Id.* at

43:57–60. In addition, Dua describes a “wallet account” that a user can set up with a mobile operator or “wallet service provider” to allow the user to store credentials, personal information, and other confidential information. *Id.* at 61:26–30. Dua explains that when a key is received by the RFID chip in the wireless device, it automatically launches the wallet application resident in the device. *Id.* at 36:63–66. The wallet application uses the key to search for and locate a specific credential for transmission back to the reader via the device’s RF capability. *Id.* at 38:66–37:2; *see also id.* at 46:31–36. The successful transmission of credential to the reader results in a tone being sounded by the wireless device. *Id.* at 38:45–47.

According to Dua, a “credential” is actual “account information or personal information,” where the account information includes, among other information, account specific information, account number, special security information related to the credential, such as CVV/CVC. *Id.* at 32:22–42.

4. Reasonable Likelihood Determination

a) Petitioner’s Burden

A petition for *inter partes* review must identify “with particularity, each claim challenged, the grounds on which the challenge to each claim is based, and the evidence that supports the grounds for the challenge to each claim.” 35 U.S.C. § 312(a)(3); *see also* 37 C.F.R. § 42.104(b) (specifying necessary elements of a petition). Further, a petition must state how a challenged claim is to be construed and how each element of the construed claim is found in prior art patents or printed publications. 37 C.F.R. §§ 42.104(b)(3)–(4).

b) *The “Identification Code” Limitations*

Each of independent claims 1 and 9 recites, in relevant part, “wherein the NFC terminal transfers the identification code to a management server which transmits the identification code to a transaction server for processing of the NFC transaction using a payment method corresponding to the identification code.” Ex. 1001, 5:65–6:3, 6:47–51. The Petition does not include an express interpretation of the claimed “identification code,” “payment method,” or any other claim language. See Pet. 11 (noting that words in a claim are generally given their plain and ordinary meaning and stating that no claim terms require construction).

Petitioner instead advances an implicit interpretation; for each challenged independent claim in each asserted ground, Petitioner contends the claims’ “identification code” limitations are satisfied by prior art disclosures of credit card numbers, expiration dates, and CVV codes. Pet. 25, 32–33, 38, 55–56, 64–65, 68–69. But because the Petition does not address the scope or meaning of “identification code,” the Petition does not explain why a “credit card’s number, its expiration date and CVV code” (Pet. 25) would fall within the scope of “identification code” as claimed.

Patent Owner asserts the claims require an “identification code” separate from the “payment method *corresponding* to the identification code.” Prelim. Resp. 22. Further, Patent Owner contends that because the claims separately recite “identification code” and “payment method,” the “identification code” must be something different than the “payment method” itself. Prelim. Resp. 22–24.

Faced with Patent Owner’s arguments, Petitioner requested additional briefing, stating “Petitioner could not have anticipated” Patent Owner’s “construction of the term ‘identification code’ as excluding payment

credentials such as a credit card number, expiration date, CVV code, and other payment information.” Ex. 3001, 2. Noting that the scope and meaning of “identification code” is potentially dispositive, the Board authorized the parties to address that issue in additional briefing. Paper 10, 2–3.

With that authorization, Petitioner filed a Reply to Patent Owner’s Preliminary Response. Paper 11 (“Reply”). Petitioner’s Reply argues Patent Owner’s position that “‘identification code’ excludes payment credentials such as credit card numbers . . . finds no support in the plain and ordinary claim language, which at least covers a server processing credit/debit card payment based on the card number stored on a mobile device and selected by the user, without restricting what the ‘identification code’ may be.” Reply 1 (emphasis omitted).

Although not cited in the Petition, Petitioner’s Reply cites portions of the specification and the prosecution history as intrinsic evidence purportedly supporting its position that “identification code” can include “payment credentials.” Reply 1–2 (citing Ex. 1001, 3:42–50, 5:32–37; Ex. 1017² pp. 422–23; Ex. 1022 ¶ 50; Ex. 2002 p. 241). But far from defining the claimed “identification code,” the cited intrinsic evidence at most describes embodiments in which some payment credentials may be stored on a mobile device in certain circumstances. And Petitioner acknowledges (Reply 2 n. 4) that the specification also describes embodiments in which payment information *is not* stored on a mobile device (Ex. 1001, 3:25–41 (“in one implementation, sensitive information (e.g.,

² References to Exhibit 1017 correspond to the record in IPR2021-01569, but the same document has been filed in this proceeding as Exhibit 1002, which we have considered as cited by Petitioner.

banking account numbers, credit card account numbers, expiry dates, and so on) are never stored on the mobile communication device”)). None of the evidence cited by Petitioner uses, much less defines, the term “identification code,” and Petitioner does not explain sufficiently why the embodiments cited in its Reply relate to the challenged claims or why the contradictory embodiments do not.

Also, although Petitioner cites statements made during prosecution regarding an RFID-based prior art reference that purportedly transmits credit card information (Reply 2 (citing Ex. 1017 pp. 422–23)), those statements regarding the prior art’s identification code do not equate to the claimed “identification code” with credit card information. Further, Petitioner noticeably does not address earlier statements from the same document in which the Applicant argued support for “identification code” comes from an application incorporated by reference that describes, for example, that initiation of a transaction causes “the transmission of the identification code associated with the secure element 130 and thus the user,” distinct from the user’s personal and credit card information stored on a server. Ex. 1002, 420. The quoted portion and others identified for support for “identification code” further undercut Petitioner’s implicit interpretation of “identification code,” and Petitioner plainly failed to adequately and accurately address these and other relevant portions of the intrinsic record. *See id.* at 420–21.

Even more problematic, Petitioner does not does not directly address in the Petition or in its Reply the fact that the claims recite both an “*identification code*” and a “*payment method that corresponds to the identification code.*” *See* Prelim. Resp. 22. The Court of Appeals for the Federal Circuit has explained that “[i]n the absence of any evidence to the contrary, we must presume that the use of . . . different terms in the claims

connotes different meanings.” *CAE Screenplates, Inc. v. Heinrich Fielder GmbH*, 224 F.3d 1308, 1317 (Fed. Cir. 2000). Patent Owner persuasively argues that the claims’ recitation of “identification code” and “payment method” as two separate elements means that the “identification code” is something different than the “payment method,” and Petitioner does not advance adequate evidence to the contrary. Prelim. Resp. 22–24; Sur-Reply 1 (“the use of two terms in a claim requires that they connote different meanings” (quoting *Applied Med. Res. Corp. v. U.S. Surgical Corp.*, 448 F.3d 1324, 1333 n.3 (Fed. Cir. 2006))). Further, Petitioner does not explain what it contends the recited “payment method” is if the claimed “identification code” includes credit card numbers, expiration dates, and CVV codes, nor does Petitioner clearly argue, much less adequately evidence, that the claim terms can include the same things. The Chatterjee Declaration also fails to explain and clearly state the distinctions we find lacking. See Chatterjee Decl. ¶¶ 135–147, ¶¶ 218–227.

Accordingly, having considered the parties’ arguments and evidence of record, we determine Petitioner has not adequately established that the claimed “identification code” should be construed to include the prior art’s teachings of credit card numbers, expiration dates, and CVV codes. Thus, we determine Petitioner has not adequately shown that the cited prior art satisfies the claims’ limitations reciting an “identification code” and a “payment method.”

Because this deficiency exists for each independent claim in each asserted ground, Petitioner has not carried its burden to show a reasonable likelihood that it would prevail with respect to at least one of the claims challenged in the Petition. We need not consider Patent Owner’s additional

arguments for purposes of deciding whether to institute a review in this Decision.

III. CONCLUSION

For the foregoing reasons, we are not persuaded that Petitioner has established a reasonable likelihood of prevailing on its assertion that any of challenged claims 1–16 of the '493 patent are unpatentable.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that the Petition is *denied*, and no trial is instituted.

IPR2021-01571
Patent 9,378,493 B2

FOR PETITIONER:

Todd M. Friedman
Jon Carter
Bao Nguyen
KIRKLAND & ELLIS LLP
todd.friedman@kirkland.com
carterj@kirkland.com
bnguyen@kirkland.com
samsung_blaze@kirkland.com

FOR PATENT OWNER:

Stephen Underwood
Jason C. Linger
GLASER WEIL FINK HOWARD AVCHEN & SHAPIRO LLP
sunderwood@glaserweil.com
jlinger@glaserweil.com