

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD.,
Petitioner,

v.

BLAZE MOBILE, INC.,
Patent Owner.

IPR2021-01570
Patent 10,565,575 B2

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

O'HANLON, *Administrative Patent Judge.*

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. Background

Samsung Electronics Co., Ltd. (“Petitioner”) filed a Petition for *inter partes* review of claims 1–30 (“the challenged claims”) of U.S. Patent No. 10,565,575 B2 (Ex. 1001, “the ’575 patent”). Paper 3 (“Pet.”), 1. Blaze Mobile, Inc. (“Patent Owner”) filed a Preliminary Response.¹ Paper 10 (“Prelim. Resp.”). With our authorization (*see* Paper 12), Petitioner filed a Preliminary Reply (Paper 13, “Prelim. Reply”) and Patent Owner filed a Preliminary Sur-reply (Paper 16, “Prelim. Sur-reply”).

Institution of an *inter partes* review is authorized by statute only when “the information presented in the petition . . . and any 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(a) (2018). We have authority, acting on the designation of the Director, to determine whether to institute an *inter partes* review under 35 U.S.C. § 314 and 37 C.F.R. § 42.4(a). For the reasons set forth below, upon considering the Petition, Preliminary Response, and evidence of record, we conclude that the information presented in the Petition fails to establish a reasonable likelihood that Petitioner would prevail in showing the unpatentability of any of the challenged claims. Accordingly, we decline to institute *inter partes* review.

¹ Although Patent Owner indicates that Michelle Fisher owns the ’575 patent (*see* Prelim. Resp. 1), Office records indicate that Ms. Fisher assigned “the entire right, title and interest” in the ’575 patent to Blaze Mobile, Inc. *See* Ex. 1002, 313.

B. Real Parties in Interest

Petitioner identifies itself and Samsung Electronics America, Inc. as real parties in interest. Pet. 2.

Patent Owner identifies itself and Michelle Fisher as real parties in interest. Paper 5, 1; Paper 11, 1; Paper 14, 1.

C. Related Matters

The parties indicate that the '575 patent is the subject of the following district court declaratory judgment action:

Samsung Electronics Co. Ltd. v. Blaze Mobile Inc., Case No. 21-cv-02989 (N.D. Cal. filed September 3, 2021).

Pet. 2; Paper 5, 1; Paper 11, 1; Paper 14, 1. Petitioner states that the complaint for the declaratory judgment action seeks a judgment of non-infringement of the '575 patent and other patents, including two patents related to the '575 patent (U.S. Patent Nos. 10,699,259 ("the '259 patent") and 10,825,007 ("the '007 patent")) and two patents unrelated to the '575 patent (U.S. Patent Nos. 9,378,493 ("the '493 patent") and 9,652,771 ("the '771 patent")). Pet. 2.

Patent Owner notes that Petitioner has filed several petitions seeking *inter partes* review of Patent Owner's patents, including those filed in IPR2021-01529, IPR2021-01530, IPR2021-01569, and IPR2021-01571. Paper 5, 1; Paper 11, 1; Paper 14, 1. We note that these petitions challenge the '259 patent, the '007 patent, the '771 patent, and the '493 patent, respectively.

D. The Challenged Patent

The '575 patent discloses “a method and system for conducting an online payment transaction through a point of sale device . . . in which the payment authorization is sent to the payment entity via a mobile communication device of the user.” Ex. 1001, 1:45–55. The mobile device may be an NFC-enabled phone. *Id.* at 3:46–47. Petitioner’s declarant testifies that “NFC is a standardized, very short range communication technology that allows devices placed in close proximity of each other (a few centimeters or less) to communicate with each other wirelessly.” Ex. 1003 ¶ 41. Figure 4 of the '575 patent, reproduced below, illustrates a communication system using an NFC-enabled phone.

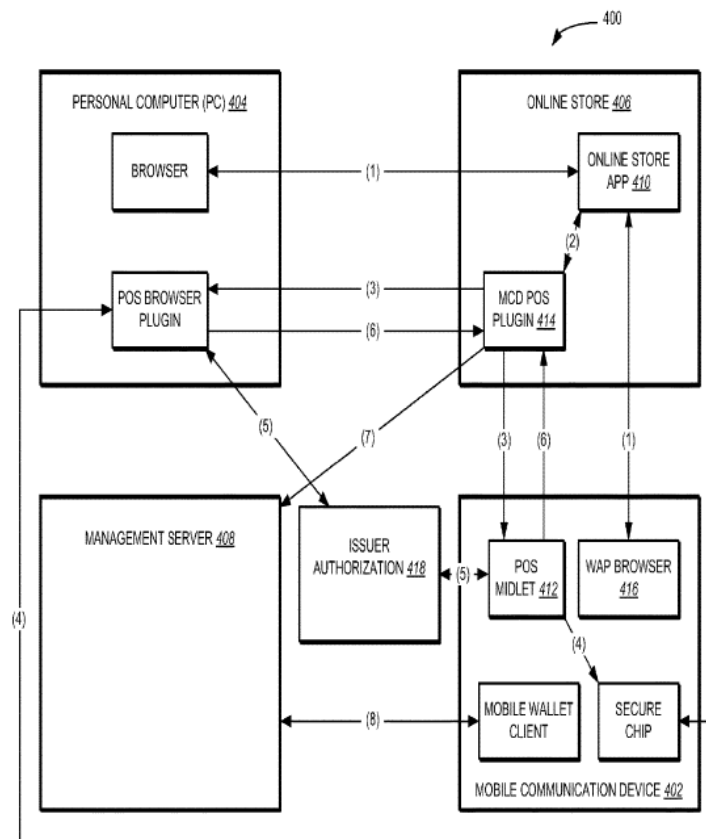


FIG. 4

Figure 4 is a block diagram of a communication system including a wireless mobile phone 402 and an online store 406. Ex. 1001, 2:25–27. The phone includes a mobile wallet application. *Id.* at 3:13–19. When a user is shopping at an online store via personal computer 404 and is ready to pay for the selected products, the user selects a payment method in the mobile wallet then waves the phone over the NFC reader on the computer. *Id.* at 3:64–4:4. The user's payment credentials are transferred from the phone to the merchant website 410 using a communication protocol between the NFC chip in the phone and the NFC chip in the computer. *Id.* at 4:4–8. The user enters any required validation information, and the purchase is processed by the merchant's online processor. *Id.* at 4:13–17.

Alternatively, the user's payment credentials are stored in a virtual wallet on management server 408. Ex. 1001, 4:59–64. The user initiates payment by entering its phone number on the merchant portal. *Id.* at 4:46–48. The management server verifies the user's identity by sending a unique code to the mobile wallet application on the user's phone, and the user enters the code onto the merchant's web portal. *Id.* at 4:52–57. The merchant's web portal sends the code to the management server to authenticate the user. *Id.* at 4:57–59. The management server then sends the user's payment information to the merchant portal. *Id.* at 4:59–64. The user enters any required validation information, and the purchase is processed by the merchant's online processor. *Id.* at 5:3–7.

E. The Challenged Claims

Petitioner challenges claims 1–30 of the '575 patent. Pet. 1, 5. Claims 1 and 14 are independent. Claim 1 is illustrative of the challenged claims and is reproduced below.

1. A method for conducting a Near Field Communication (NFC) transaction using an NFC protocol, the method comprising:

maintaining a non-browser based application in a mobile device memory, wherein the non-browser based application is a mobile operating system platform non-browser based mobile application with a graphical user interface that is preinstalled or downloaded and installed on a mobile device, the mobile device comprising the mobile device memory, a mobile device display, a mobile device processor, a mobile device wireless transceiver that supports voice and data interactions through a first communication channel, an NFC transceiver configured to use the NFC protocol through a second communication channel, an NFC processor configured to use the NFC protocol, and a secure element memory, wherein the secure element memory maintains an identification code associated with a user and a secure element application configured to use the NFC protocol, wherein the secure element memory, NFC transceiver, and NFC processor are included in a secure element permanently embedded within a body of the mobile device, wherein the graphical user interface includes a graphical icon;

executing the secure element application in response to a detection of a near field communication inductive signal from an NFC terminal configured to use the NFC protocol; and

transmitting, using the secure element application, via the NFC transceiver, first transaction information including the identification code associated with the user via the second communication channel from the secure element memory to the NFC terminal during an NFC inductive interaction between the secure element and the NFC terminal, wherein

the first transaction information including the identification code associated with the user is transmitted to a remote management server which transmits second transaction information including a payment method that corresponds to the identification code associated with the user to a transaction server that processes the NFC transaction using the payment method that corresponds to the identification code associated with the user, wherein the payment method is maintained at the remote management server; and

after the NFC transaction has been processed, receiving, at the mobile device, a digital artifact for display in the graphical user interface of the non-browser based application.

Ex. 1001, 7:48–8:29.

F. Asserted Grounds of Unpatentability

The Petition relies on the following prior art references:

Name	Reference	Exhibit
Huomo	WO 2006/095212 A1, published September 14, 2006	1005
Sklovsky	US 2008/0162312 A1, published July 3, 2008	1006
Dua	US 8,700,729 B2, April 15, 2014	1008

Petitioner asserts the following grounds of unpatentability:

Claim(s) Challenged	35 U.S.C. §	Reference(s)
1–30	103(a) ²	Huomo, Dua
1–30	103(a)	Sklovsky, Dua

² The application resulting in the '575 patent claims priority to a date prior to when the Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112–29, 125 Stat. 284 (2011), took effect. Thus, we refer to the pre-AIA version of section 103.

Pet. 5. Petitioner submits a declaration of Sandeep Chatterjee, Ph.D. (Ex. 1003, “Chatterjee Declaration”) in support of its contentions. Patent Owner submits a declaration of Michelle Fisher (Ex. 2007) in support of its preliminary responses.

II. ANALYSIS

A. Principles of Law

“In an [*inter partes* review], the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable.” *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) (requiring *inter partes* review petitions to identify “with particularity . . . the evidence that supports the grounds for the challenge to each claim”)). Petitioner bears the burden of persuasion to prove unpatentability of each challenged claim by a preponderance of the evidence. 35 U.S.C. § 316(e). This burden never shifts to Patent Owner. *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015). The Board may authorize an *inter partes* review if we determine that the information presented in the Petition and Patent Owner’s Preliminary Response shows that there is a reasonable likelihood that Petitioner will prevail with respect to at least one of the claims challenged in the petition. 35 U.S.C. § 314(a).

A patent claim is unpatentable under 35 U.S.C. § 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 the 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, any objective evidence of nonobviousness.³ *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

B. 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.* (internal quotation marks and citation omitted).

Petitioner contends that a person having ordinary skill in the art at the time of the 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.” Pet. 9 (citing Ex. 1003 ¶ 34). Petitioner contends that

³ At this stage of the proceeding, the parties have not directed us to any such objective evidence.

“[a]dditional education might compensate for less experience, and vice-versa.” *Id.*

Patent Owner contends that a person having ordinary skill in the art at the time 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. 8.

The parties do not identify, and we do not discern, any material difference between the parties’ proposed definitions. For purposes of this decision and based on the record currently before us, we adopt Petitioner’s proposed definition of the level of ordinary skill. We note that we would reach the same conclusions under either proposed standard.

C. Claim Construction

In an *inter partes* review, claims are construed using the same claim construction standard that would be used to construe the claims in a civil action under 35 U.S.C. § 282(b), including construing the claims in accordance with the ordinary and customary meaning of such claims as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent. 37 C.F.R. § 42.100(b). Thus, we apply the claim construction standard as set forth in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). In addition to the specification and prosecution history, we also consider use of the terms in other claims and extrinsic evidence including expert and inventor testimony, dictionaries, and learned treatises, although extrinsic evidence is less significant than the intrinsic record. *Id.* at 1312–17. Usually, the specification is dispositive, and it is the single best guide to the meaning of a disputed term. *Id.* at 1315.

Only those terms that are in controversy need be construed, and only to the extent necessary to resolve the controversy. *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)).

Neither Petitioner nor Patent Owner proposes definitions for any claim terms. *See, e.g.*, Pet. 9. For purposes of this Decision, and based on the record before us, we determine that no construction of any term is necessary.

D. Overview of the Asserted Prior Art

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. Ex. 1005, 4:12–14. Smartcards provide a secure environment for storing items of monetary value and can be used in conjunction with the contactless features of near field communications. *Id.* at 3:9–11. In use, the smartcard module is activated, which can be done via a graphical user interface. *Id.* at 4:14–16, 5:8–9. Then it is determined whether the smartcard application

is for data transactions with external entities and, if so, a connection is made between the smartcard module and the near field communication module.

Id. at 4:19–22. Figure 2a illustrates a schematic arrangement of the smartcard and NFC modules and is reproduced below.

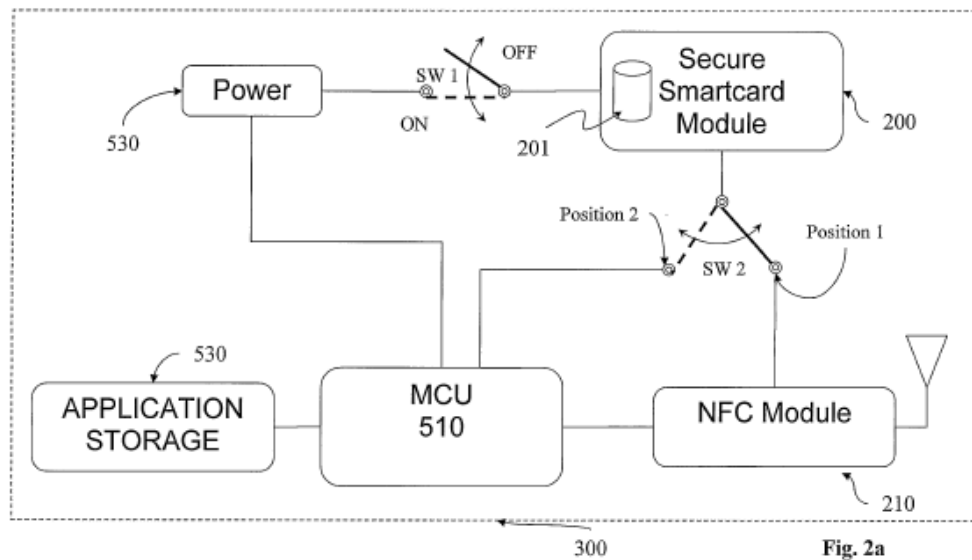


Figure 2a shows an exemplary schematic arrangement of smartcard module 200 and NFC module 210, as well as other elements of a mobile device. *Id.* at 12:29–31. Smart card module 200 is integrated into the mobile device and includes secure storage area module 201. *Id.* at 13:2–5. Huomo explains that “secure storage module 201 may be used for storing different data in a tamperproof environment on the smartcard.” *Id.* at 13:5–6. Secure smart card module 200 is connected to power source 530 via user controllable power switch SW1. *Id.* at 13:7–9. The smartcard module is inactive unless switch SW1 is closed to ensure security and prevent unauthorized access to the smartcard, including its secure storage module. *Id.* at 12:10–23, 14:6–20. Switch SW2 connects secure smart card element 200 to either Near Field Communication interface 210 to provide connectivity with external devices or to terminal mobile control unit

(MCU) 510 for control of smart card element 200 to, for example, view information relating to conducted transactions. *Id.* at 13:9–13, 15:22–31. Use of the smartcard module may require authorization, which “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. Huomo further describes an embodiment in which a mobile terminal receives a receipt after a transaction is performed, which can be stored in special storage within the smartcard module. *Id.* at 21:10–17.

2. Sklovsky

Sklovsky relates to contactless transactions using a mobile device, such as contactless credit card transactions with a reader terminal using Near Field Communication (NFC) technology. Ex. 1006 ¶¶ 2–3. Sklovsky discloses that known systems use a secure module on the user’s mobile device to transmit stored credit card information to the reader terminal, but the user may not have any means of detecting whether the credit card information was received by the reader terminal. *Id.* ¶ 5. Sklovsky purports to improve such known systems by providing a system that monitors secure contactless transaction events in a mobile device. *Id.* ¶¶ 11, 32. The system includes a secure controller that monitors state transitions generated in response to an execution of events between an NFC modem and an NFC reader. *Id.* ¶¶ 32, 35. A state transition can be a request to make a payment,

enable a payment, confirm a payment, or cancel a payment. *Id.* ¶¶ 35, 46. The secure controller sends event notifications to the mobile host, which provides the information to the mobile device user through the mobile device user interface resources, such as the display. *Id.* ¶¶ 35–36. Figure 4, reproduced below, illustrates the secure controller.

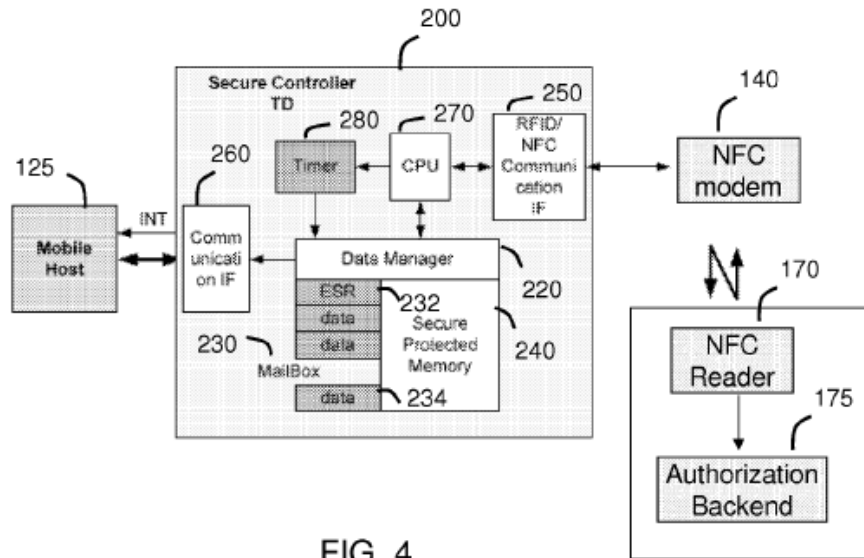


FIG. 4

Figure 4 is a block diagram of secure controller 200 for a contactless transaction system. *Id.* ¶ 43. The secure controller 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 the communication interface for handling event notifications. *Id.* The data manager can include secure protected memory 240 for storing data and transaction events between NFC modem 140 and NFC reader 170, and mailbox 230 for retrieving the data and transaction events and providing event notifications to communication interface 260, which sends messages regarding event notifications to mobile host 125. *Id.* ¶¶ 43–44.

In operation, the secure controller detects event execution by monitoring the state transitions that are associated with events. Ex. 1006 ¶ 46. The NFC reader sends a transaction acknowledgement to the NFC modem upon completing a contactless transaction. *Id.* ¶ 47. The NFC modem receives the acknowledgement and the controller sets a flag to notify the mobile host of an event. *Id.* ¶ 48. The mobile host receives the notification and displays information associated with the contactless transaction for the user to view. *Id.* ¶ 49.

3. *Dua*

Dua discloses “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 system uses a wallet application, which “is a platform capable of securely holding a myriad of different electronic credentials and making them available in a controlled way through specific functions.” Ex. 1008, 31:8–11. A credential is the actual account information that is transmitted by an issuer, such as a credit card company. *Id.* at 32:22–24. Rather than using a credit card, a user can utilize a mobile device with a wallet application to conduct a transaction. *Id.* at 33:23–24. During the transaction process, the wireless device transmits payment information to a reader using the short-range transmission capability of the wireless device. *Id.*

at 33:25–28. Typically, the user must enter a personal identification number code to authenticate the user to the application. *Id.* at 39:1–6.

Rather than being located on the user’s mobile device, a wallet account can be hosted by a wallet service provider. Ex. 1008, 61:26–28. This server-based wallet account allows the user to access “the entire ‘electronic wallet’ from virtually any Internet-based channel.” *Id.* at 61:32–45. In this embodiment, the wallet server transmits the user’s credentials to the point of sale system for processing. *Id.* at 64:17–20.

E. Asserted Obviousness Based on Huomo and Dua

Petitioner argues that claims 1–30 would have been obvious over Huomo and Dua. Pet. 19–52. In support of its showing, Petitioner relies upon the Chatterjee Declaration. *Id.* (citing Ex. 1003). We have reviewed Petitioner’s assertions and supporting evidence. For the reasons discussed below, and based on the record before us, we determine that Petitioner does not demonstrate a reasonable likelihood of prevailing in showing that at least one challenged claim would have been obvious over the combination of Huomo and Dua.

Petitioner relies on Huomo to disclose a method substantially as recited in claim 1, and relies on Dua to teach the use of a server-based wallet account. Pet. 19–40. Petitioner relies on its mapping for claim 1 to challenge claim 14. *Id.* at 48–49.

Each of independent claims 1 and 14 recites a remote management server that transmits a payment method to a transaction server that processes an NFC transaction using the payment method. Ex. 1001, 8:15–22, 9:43–50. Petitioner relies on Dua to teach these recitations, mapping the wallet service

provider's server to the recited remote management server and the credit card issuer's server to the recited transaction server. Pet. 37–38 (citing Ex. 1008, 45:53–60, 61:33–45, Fig. 8; Ex. 1003 ¶ 132).

Patent Owner argues that the Petition's combination of Huomo and Dua fails because it does not show an NFC transaction processed at a transaction server as recited; rather, Patent Owner argues, each of Huomo and Dua discloses the NFC transaction being processed at the point-of-sale (“POS”) terminal. Prelim. Resp. 37–40 (citing Ex. 1005, 18:14–17, 18:19–20, 18:25–28, 21:24–30, Figs. 3, 4a; Ex. 1008, 63:7–9, 63:22–23, 64:15–25).

As noted above, Petitioner relies on Dua alone to teach the recited servers. Pet. 37–38. Dua discloses that a transaction using its server-based wallet begins with the user entering its phone number and authentication information into the POS terminal. Ex. 1008, 63:39–41. The POS terminal forwards this captured information to a wireless credential manager (“WCM”) connected to the store's network. *Id.* at 63:42–44. The WCM establishes a secure peer-to-peer session with the wallet service provider's server. *Id.* at 63:44–52. The WCM sends the data captured at the POS terminal to the wallet server, which validates that the user's account is in good standing. *Id.* at 63:55–59. The wallet server then transmits a menu showing all of the user's credential types, which the POS terminal displays to the user. *Id.* at 63:60–64:9. The user selects the payment method for the transaction via the POS terminal display. *Id.* at 64:10–12. “The credentials are then securely transmitted from the wallet server to the . . . WCM[,], which routes them to the POS system for processing.” *Id.* at 64:17–20. The

POS system processes payment and completes the transaction. *Id.* at 64:20–21.

Thus, we agree that Dua discloses the POS terminal, rather than a credit card issuer's server, processes the transaction. The portions of Dua cited by Petitioner fail to explain how Dua processes the transaction other than at the POS terminal. *See* Pet. 38 (citing Ex. 1008, 45:53–60, 61:33–45, Fig. 8). The disclosure at column 45, lines 53–60 states that PINs and biometrics offer better identity validation than signatures, and the disclosure at column 61, lines 33–45 states that the server-based wallet allows the user to access the wallet from virtually any Internet-based channel. Figure 8 illustrates an over-the-air method for verifying a user's identification information in which credential information is sent from the POS terminal to the credit issuer for authorization via a first communication channel and a request for the user's personal identification number is sent from the credit issuer to the user's wireless device via a second communication channel. Ex. 1008, 43:40–50. None of the cited disclosure, however, discusses a credit card issuer's server processing a transaction. The testimony of Petitioner's declarant mirrors the arguments presented in the Petition and likewise fails to apprise us of how Dua teaches processing the transaction other than at the POS terminal. *See* Ex. 1003 ¶ 132; Pet. 38 (citing same).

Each of independent claims 1 and 14 also recites that the mobile device receives a digital artifact for display in the graphical user interface of the non-browser based application. Ex. 1001, 8:26–29, 9:24–26. Petitioner maps Huomo's "software that authenticates the user prior to activating the device's secure smartcard module" (Pet. 25 (citing Ex. 1005, 5:8–9, 17:10–14; Ex. 1003 ¶ 98)) and "[t]he combination of Huomo's

authentication software and a secure mobile payment application” (*id.* at 26 (citing Ex. 1003 ¶¶ 100–101)) to the recited non-browser based application.

Petitioner maps Huomo’s receipt to the recited digital artifact. *Id.* at 39.

Petitioner asserts that “Huomo . . . teaches that ‘the user is capable of viewing [the receipts] by means of a graphical user interface[.]’” *Id.* at 40 (alterations in original) (citing Ex. 1005, 15:29–31; Ex. 1003 ¶ 137).

However, the Petition does not explain adequately how Huomo’s “authentication software” alone or in combination with the mobile payment application (that is, the asserted non-browser based application) would display the receipt. The testimony of Petitioner’s declarant mirrors the assertions made in the Petition and likewise fails to apprise us of how Huomo’s mobile device receives the receipt for display in the graphical user interface of a non-browser based application. *See* Ex. 1003 ¶ 137; Pet. 40 (citing same).

For at least the foregoing reasons, Petitioner fails to demonstrate a reasonable likelihood of prevailing on its assertion that claims 1 and 14 would have been unpatentable as obvious over Huomo and Dua. Because of their dependence from claims 1 and 14, we further determine that Petitioner has also failed to demonstrate a reasonable likelihood of prevailing on its assertion that claims 2–13 and 15–30 would have been unpatentable as obvious over Huomo and Dua.

F. Asserted Obviousness Based on Sklovsky and Dua

Petitioner argues that claims 1–30 would have been obvious over Sklovsky and Dua. Pet. 52–86. In support of its showing, Petitioner relies upon the Chatterjee Declaration. *Id.* (citing Ex. 1003). We have reviewed

Petitioner's assertions and supporting evidence. For the reasons discussed below, and based on the record before us, we determine that Petitioner does not demonstrate a reasonable likelihood of prevailing in showing that at least one challenged claim would have been obvious over the combination of Sklovsky and Dua.

Petitioner relies on Sklovsky to disclose a method substantially as recited in claim 1, and relies on Dua to teach the use of a server-based wallet account. Pet. 52–76. Petitioner relies on its mapping for claim 1 to challenge claim 14. *Id.* at 85.

As noted above, each of independent claims 1 and 14 recites a remote management server that transmits a payment method to a transaction server that processes an NFC transaction using the payment method. Ex. 1001, 8:15–22, 9:43–50. Petitioner relies on Dua to teach these recitations in the same manner as in the challenge based on Huomo and Dua, mapping Dua's wallet service provider's server to the recited remote management server and the credit card issuer's server to the recited transaction server. Pet. 73–74 (citing Ex. 1008, 45:53–60, 61:33–45, Fig. 8; Ex. 1003 ¶¶ 240–241). However, for the reasons set forth in § II.E above, the Petition and Petitioner's declarant fail to explain adequately how Dua processes the transaction other than at the POS terminal.

As also noted above, each of independent claims 1 and 14 recites that the mobile device receives a digital artifact for display in the graphical user interface of the non-browser based application. Ex. 1001, 8:26–29, 9:24–26. Petitioner maps “Sklovsky's contactless applications” to the recited non-browser based application. Pet. 58–59 (citing Ex. 1006 ¶¶ 7, 16, 36–38, 60, Fig. 9; Ex. 1003 ¶¶ 196–198). Petitioner maps Dua's digital receipt to the

recited digital artifact. *Id.* at 75–76. Petitioner asserts that Dua teaches “that the digital receipt would appear ‘in the display of the wireless device running the wallet application.’” *Id.* at 76 (citing Ex. 1008, 48:64–67, 49:23–25, 49:40–56, 50:20–24). However, Petitioner relies on Dua’s *server-based* wallet application in its earlier mappings of claim 1. *See, e.g., id.* at 73–74. Petitioner does not explain adequately its seemingly incompatible reliance on Dua’s server-based wallet for its mapping of the recited management server and its reliance on Dua’s mobile device-based wallet for its mapping of the recited digital artifact.

For at least the foregoing reasons, Petitioner fails to demonstrate a reasonable likelihood of prevailing on its assertion that claims 1 and 14 would have been unpatentable as obvious over Sklovsky and Dua. Because of their dependence from claims 1 and 14, we further determine that Petitioner has also failed to demonstrate a reasonable likelihood of prevailing on its assertion that claims 2–13 and 15–30 would have been unpatentable as obvious over Sklovsky and Dua.

G. Discretionary Denial Under 35 U.S.C. § 325(d)

Patent Owner argues that we should deny the challenge based on *Huomo* and *Dua* because substantially the same prior art and arguments advanced by Petitioner were presented during prosecution of the application resulting in the ’575 patent. Prelim. Resp. 11–29. Because we determine that the Petition fails to set forth a reasonable likelihood that Petitioner would prevail with respect to any of its challenges to the ’575 patent, we do not reach Patent Owner’s argument that we should exercise discretion under § 325(d) to deny institution.

III. CONCLUSION

For the foregoing reasons, we are not persuaded that the Petition establishes a reasonable likelihood that Petitioner would prevail in any of its challenges to claims 1–30 of the '575 patent.

IV. ORDER

In consideration of the foregoing, it is hereby ordered that the Petition is *denied*, and no trial is instituted.

IPR2021-01570
Patent 10,565,575 B2

For PETITIONER:

Todd M. Friedman
Jon R. Carter
Bao Nguyen
KIRKLAND & ELLIS LLP
todd.friedman@kirkland.com
jon.carter@kirkland.com
bao.nguyen@kirkland.com
Samsung_Blaze_IPR@kirkland.com

For PATENT OWNER:

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