

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD. AND
SAMSUNG ELECTRONICS AMERICA, INC.

Petitioners,

v.

MAXELL, LTD.,
Patent Owner

Case: IPR2025-01313

U.S. Patent No. 10,783,228

**PATENT OWNER'S PRELIMINARY RESPONSE
TO PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 10,783,228**

Mail Stop **Patent Board**
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. BACKGROUND	2
A. U.S Patent No. 10,783,228.....	2
B. ’228 Patent Prosecution History.....	6
C. Person Of Ordinary Skill In The Art.....	6
D. Summary Of Petitioners’ Proposed Grounds Of Unpatentability And The References Cited	7
1. Aminzade (EX1004)	7
III. LEGAL STANDARD	9
IV. PETITIONER’S EXPERT DECLARATION IS ATTORNEY ARGUMENT PRESENTED IN THE CLOTH OF EXPERT TESTIMONY	10
V. CLAIM CONSTRUCTION	14
VI. THE BOARD SHOULD DENY INSTITUTION IN VIEW OF SAMSUNG’S INDICATION THAT IT IS NOT LIMITED TO ASSERTING A DIFFERENT CLAIM CONSTRUCTION OF ANY CLAIM TERM FOR ANY OTHER PURPOSE.....	21
VII. THE PETITION DOES NOT SHOW A REASONABLE LIKELIHOOD OF PREVAILING WITH RESPECT TO ANY CHALLENGED CLAIM	26
A. Ground 1: Petitioners Fail To Establish That Claims 1-2, 4-7, 12-13, and 15-18 are Rendered Obvious By Aminzade in View of Sowers.....	26
1. No Motivation to Combine Aminzade with Sowers.....	27
2. The Combination of Aminzade and Sowers Fails to Disclose Limitation [1.c] and [12.f].....	33

TABLE OF CONTENTS
(continued)

	Page
3. The Combination of Aminzade and Sowers Fails to Disclose Limitation [1.d] and [12.g].....	38
4. The Combination of Aminzade and Sowers Fails to Disclose Limitation [1.e] and [12.h]	40
5. The Combination of Aminzade and Sowers Fails to Disclose Claims 7 and 18.....	44
B. Ground 2: Petitioners Fail To Establish That Claims 1-2, 4-7, 12-13, and 15-18 are Rendered Obvious By Aminzade in View of Soli	45
1. No Motivation to Combine Aminzade with Soli	45
2. The Combination of Aminzade and Soli Fails to Disclose Limitation [1.c] and [12.f]	51
3. The Combination of Aminzade and Soli Fails to Disclose Limitation [1.d] and [12.g].....	52
4. The Combination of Aminzade and Soli Fails to Disclose Limitation [1.e] and [12.h].....	53
5. The Combination of Aminzade and Soli Fails to Disclose Claims 7 and 18.....	54
C. Ground 3: Petitioners Fail To Establish That Claims 3, 10-11, 14, 21-22 are Rendered Obvious By Aminzade in View of Sowers and Hong.....	55
1. No Motivation to Combine Aminzade with Hong	56
D. Ground 4: Petitioners Fail To Establish That Claims 3, 10-11, 14, 21-22 are Rendered Obvious By Aminzade in View of Soli and Hong	57
E. Ground 5: Petitioners Fail To Establish That Claims 8-9, 19-20 are Rendered Obvious By Aminzade in View of Sowers and Altman	58

TABLE OF CONTENTS
(continued)

	Page
1. No Motivation to Combine Aminzade with Altman	58
F. Ground 6: Petitioners Fail To Establish That Claims 8-9, 19-20 are Rendered Obvious By Aminzade in View of Soli and Altman	63
VIII. CONCLUSION.....	64

TABLE OF AUTHORITIES

	Page(s)
 Cases	
<i>KSR Int’l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007).....	9
<i>Graham v. John Deere Co. of Kansas City</i> , 383 U.S. 1 (1966).....	9
<i>Intelligent Bio-Systems, Inc. v. Illumina Cambridge Ltd.</i> , 821 F.3d 1359 (Fed. Cir. 2016)	9
<i>Medichem, S.A. v. Rolabo, S.L.</i> , 437 F.3d 1157 (Fed. Cir. 2006)	9
<i>Cardiacom, LLC v. Bosch Healthcare Sys., Inc.</i> , IPR2013-00439, Paper 26 (P.T.A.B. Jan. 16, 2014)	12
<i>Kinetic Techs., Inc. v. Skyworks Solutions, Inc.</i> , IPR2014-00529, Paper 8 (P.T.A.B. Sept. 23, 2014).....	12
<i>In re Kahn</i> , 441 F.3d 977, 988 (Fed. Cir. 2006)	12
<i>TRW Auto. US LLC v. Magna Elecs., Inc.</i> , IPR2014- 00258, Paper 18 (P.T.A.B. Aug. 27, 2014).....	12
<i>InfoBionic, Inc. v Braemar Manufacturing, LLC.</i> , IPR2015-01704, Paper 11 (P.T.A.B. Feb. 16, 2016).....	13, 20, 31, 50, 57, 62
<i>Xerox Corp. et al. v. Bytemark, Inc.</i> , IPR2022-00624, Paper 12 (P.T.A.B. Feb. 10, 2023).....	13
<i>Samsung Elec. Am. Inc. v. Maxell Ltd.</i> , IPR2024-00735, Paper 38 (P.T.A.B. Sep. 14, 2025).....	24-25
<i>Samsung Elec. Am. Inc. v. Maxell Ltd.</i> , IPR2024-000828, Paper 39 (P.T.A.B. Sep. 15, 2025).....	25

Case IPR2025-01313
Patent No. 10,783,228
Patent Owner’s Preliminary Response

<i>Revvo Technologies, Inc. v. Cerebrum Sensor Technologies, Inc.</i> , IPR2025-00632, Paper 20 (Squires November 3, 2025).....	25
--	----

<i>American Airlines, Inc. et al v. Intellectual Ventures I LLC</i> , IPR2025-01055, Paper 11 (November 21, 2025).....	25
---	----

<i>In re Klein</i> , 647 F.3d 1343 (Fed. Cir. 2011)	27, 29, 46-47, 59-60
--	----------------------

<i>In re Nuvasive, Inc.</i> , 842 F.3d 1376 (Fed. Cir. 2016)	31, 50, 56, 62
---	----------------

<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005)	40
--	----

Statutes

35 U.S.C. § 103(a)	9
35 U.S.C. § 112	22

Other Authorities

37 C.F.R. § 42.65(a).....	1, 14, 20, 31, 50, 57, 62
37 C.F.R. § 42.104(b)(3).....	24, 26

PATENT OWNER’S EXHIBIT LIST

Description	Exhibit #
Notice Letter to Samsung (July 7, 2021)	2001
Follow-up Notice Letter to Samsung (December 29, 2021)	2002
Docket Navigator Time to Trial Statistics for the Eastern District of Texas	2003
Docket Control Order, <i>Maxell, Ltd. v. Samsung Elecs. Co., Ltd.</i> , No. 5:25-cv-00052-RWS (E.D. Tex.)	2004
Jury Trial Transcript, Vol. 4, <i>Maxell, Ltd. v. Samsung Elecs. Co., Ltd.</i> , No. 5:23-cv-00092-RWS (E.D. Tex.)	2005
Complaint, <i>Maxell, Ltd. v. Samsung Elecs. Co., Ltd.</i> , No. 5:25-cv-00052-RWS (E.D. Tex.)	2006
Follow-up Notice Letter to Samsung (September 8, 2023)	2007
Law360 Article, “Maxell Settles Patent Suit Against Apple Over Mobile Tech”	2008
Law360 Article, “Maxell Scores \$43M EDTX Jury Win In ZTE Patent Trial”	2009
Law360 Article, “Maxell, Huawei Reach Terms To End Smartphone Patent Suit”	2010
Hudson Institute Article, “Google’s Loss to Sonos Settles It, Big Tech Has an IP Piracy Problem”	2011
PatentRenewal.com Article, “which-companies-hold-the-most-patents-in-the-world”	2012
Motion for Partial Summary Judgment of Validity Based on Sotera Stipulations, <i>Maxell, Ltd. v. Samsung Elecs. Co., Ltd.</i> , No. 5:23-cv-00092-RWS (E.D. Tex.)	2013
Follow-up Notice Letter to Samsung (November 28, 2024)	2014
Defendants’ P.R. 3-3 and 3-4 Invalidity Contentions and Disclosures, <i>Maxell, Ltd. v. Samsung Elecs. Co., Ltd.</i> , No. 5:25-cv-00052-RWS (E.D. Tex.)	2015

Case IPR2025-01313
Patent No. 10,783,228
Patent Owner's Preliminary Response

Samsung, “Unable to unlock Galaxy’s phone or tablet’s screen”	2016
Samsung, “Lock and Unlock Samsung DeX”	2017
U.S. Patent No. 8,745,379 (the “’379 Patent”)	2018

LISTING OF CHALLENGED CLAIMS¹

Claim	Claim Text
[1.pre]	A system, comprising:
[1.a]	a first information processing device including:
[1.a.i]	a dynamic biometric information acquisition sensor that acquires dynamic biometric information from a body of a user; and
[1.a.ii]	a first communication interface that transmits the acquired dynamic biometric information; and
[1.b]	a second information processing device including:
[1.b.i]	a static biometric information acquisition sensor that acquires static biometric information;
[1.b.ii]	a processor that performs user authentication based on the acquired static biometric information and obtains an authentication result;
[1.b.iii]	a second communication interface that performs communication relating to the authentication result with the first communication interface and receives the dynamic biometric information transmitted from the first communication interface; and
[1.b.iv]	a display screen,
[1.c]	wherein the first information processing device: performs communication relating to the authentication result between the first communication interface and the second communication interface and executes an unlock operation to unlock itself in response to the communication relating to the authentication result,

¹ For convenience purposes only, Patent Owner adopts for this Preliminary Response the numbering of claim elements advanced by Petitioners in the Petition. Patent Owner does not concede the appropriateness of such grouping and numbering of claim elements.

[1.d]	acquires the dynamic biometric information from the dynamic biometric information acquisition sensor after unlocking, and
[1.e]	maintains the unlocked state during a condition that the dynamic biometric information can be acquired,
[1.f]	wherein the second information processing device receives the dynamic biometric information via communication between the first communication interface and the second communication interface and the display screen displays information based on a state of the user that is determined using the received dynamic biometric information.
[2]	The system according to claim 1, wherein the first communication interface and the second communication interface are Bluetooth interfaces and communication between the first communication interface and the second communication interface is Bluetooth wireless communication.
[3]	The system according to claim 1, wherein the first communication interface and the second communication interface are Wi-Fi interfaces and communication between the first communication interface and the second communication interface includes establishing a Wi-Fi Direct connection.
[4]	The system according to claim 1, wherein the dynamic biometric information is one of heart rate, pulse, blood pressure, body temperature, amount of sweating, or brain wave and the static biometric information is one of finger print information, facial recognition information, retina information, vein information, or iris information.
[5]	The system according to claim 1, wherein the first information processing device is a wearable device that acquires the dynamic biometric information at least by being physically in contact with the body.

[6]	The system according to claim 1, wherein the first information processing device is a smartwatch and the second information processing device is a smartphone or tablet.
[7]	The system according to claim 1, wherein the first information processing device continuously acquires the dynamic biometric information after being unlocked and the second information processing device receives the dynamic biometric information transmitted from the first communication device continuously or based on starting of an application on the second information processing device.
[8]	The system according to claim 1, wherein the second information processing device gets position information denoting a position of the second information processing device and automatically transmits the position information to a predetermined address based on reception of a user input that is determined to be a predetermined type of user input during a time period, wherein the predetermined address is not inputted by the user during the time period.
[9]	The system according to claim 8, wherein the position information is automatically transmitted in response to the user input and without requiring additional user input that explicitly requires approval of the automatic transmission of the position information during the time period.
[10]	The system according to claim 1, wherein upon determining that the user is in a state matching predetermined criteria, the second information processing device limits an operation of the second information processing device by displaying a screen seeking confirmation from the user that the user intended to execute the operation.
[11]	The system according to claim 10, wherein the operation is executed on the second information processing device after the user provides confirmation in response to displaying of the screen.

[12.pre]	A method, comprising:
[12.a]	acquiring dynamic biometric information from a body of a user by a dynamic biometric information acquisition sensor of a first device;
[12.b]	transmitting the acquired dynamic biometric information through a first communication interface of the first device to a second device;
[12.c]	acquiring static biometric information by a static biometric information acquisition sensor of the second device;
[12.d]	performing user authentication to obtain an authentication result based on the acquired static biometric information;
[12.e]	performing communication with a second communication interface relating to the authentication result with the first communication interface and receiving the dynamic biometric information transmitted from the first communication interface;
[12.f]	performing communication relating to the authentication result between the first communication interface and the second communication interface and executing an unlock operation to unlock the first device in response to the communication relating to the authentication result,
[12.g]	acquiring the dynamic biometric information from the dynamic biometric information acquisition sensor of the first device after unlocking, and
[12.h]	maintaining the unlocked state during a condition that the dynamic biometric information can be acquired;
[12.i]	receiving the dynamic biometric information by the second device via communication between the first communication interface and the second communication interface; and
[12.j]	displaying on a display screen information based on a state of the user that is determined using the received dynamic biometric information.

[13]	The method according to claim 12, wherein the first communication interface and the second communication interface are Bluetooth interfaces and the communication performed between the first communication interface and the second communication interface is Bluetooth wireless communication.
[14]	The method according to claim 12, wherein the first communication interface and the second communication interface are Wi-Fi interfaces and the communication performed between the first communication interface and the second communication interface includes establishing a Wi-Fi Direct connection.
[15]	The method according to claim 12, wherein the acquiring of dynamic biometric information acquires one of heart rate, pulse, blood pressure, body temperature, amount of sweating, or brain wave and the static biometric information is one of finger print information, facial recognition information, retina information, vein information, or iris information.
[16]	The method according to claim 12, wherein the acquiring of dynamic biometric information by the acquisition sensor of the first device acquires the dynamic biometric information with a wearable device at least by being physically in contact with the body.
[17]	The method according to claim 12, wherein the dynamic biometric information is acquired by a smartwatch as the first device and the dynamic biometric information acquired by a smartphone or tablet as the second device.
[18]	The method according to claim 12, wherein the dynamic biometric information is continuously acquired by the first device after being unlocked and the second device receives the dynamic biometric information transmitted from the first device continuously or based on starting of an application on the second device.

[19]	The method according to claim 12, wherein the second device gets position information denoting a position of the second device and automatically transmits the position information to a predetermined address based on reception of a user input that is determined to be a predetermined type of user input during a time period, wherein the predetermined address is not inputted by the user during the time period.
[20]	The method according to claim 19, wherein the position information is automatically transmitted in response to the user input and without requiring additional user input that explicitly requires approval of the automatic transmission of the position information during the time period.
[21]	The method according to claim 12, wherein upon determining that the user is in a state matching predetermined criteria, the second device limits an operation of the second device by displaying on the display screen a message seeking confirmation from the user that the user intended to execute the operation.
[22]	The method according to claim 21, wherein the operation is executed on the second device after the user provides confirmation in response to the displaying of the message on the display screen.

I. INTRODUCTION

Patent Owner Maxell, Ltd. ("Patent Owner") respectfully requests that the Board deny institution because Petitioners Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (hereinafter "Petitioner" or "Samsung") has failed to demonstrate a reasonable likelihood of success on the grounds submitted in its Petition for challenging the patentability of claims 1-22 ("challenged claims") of U.S. Patent No. 10,783,228 ("the '228 Patent") (EX1001).

Petitioners fail to show a reasonable likelihood of prevailing on any Ground because it has not shown that the cited references render obvious claims 1-22. None of the cited references alone or in combination disclose the arrangement of each element of claims 1-22. For example, Aminzade fails to disclose an "unlock" function according to the plain and ordinary meaning of the term in the context of the '228 Patent. *See* § VII.A.2.

Moreover, the Petition is filled with conclusory statements that fail to demonstrate a reasonable likelihood of success on any ground and are neither bolstered nor supported by Dr. Seth Nielsen's declaration (EX1003), which simply parrots Petitioners' conclusions without additional analysis or evidence. *See* 37 C.F.R. § 42.65(a) ("Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.").

For at least these reasons, Petitioners have failed to meet their burden of showing a reasonable likelihood of prevailing. Accordingly, the Director should deny Petitioners' request to institute *inter partes* review.

II. BACKGROUND

A. U.S Patent No. 10,783,228

The '228 Patent is entitled "Information Processing Device, Application Software Start-up System, and Application Software Start-up Method," and claims priority to U.S. Patent application 15/315,735, filed on June 12, 2014. The '228 Patent issued on September 22, 2020.

The '228 Patent is directed to an application software start-up system that includes a first device in communication with a second device, whereby the application software that is started up on the second device is limited depending on the state of the user, wherein the state of the user is determined by a method comparing dynamic biological information acquired from the body of the user through the first device. EX1001, at 1:54-2:21. This start-up system functions to limit access to application software by detecting a user's "emotional biometrics," particularly in circumstances in which the user may be "threatened" or "forced to perform an illegal operation." *Id.* at 1:54-60.

At the time of invention, existing biometrics authentication systems used static biometrics, which could not read a user's "intension" or emotional state. *Id.* at

1:15-19. This could lead to circumstances where, for instance, “when the user is involved in a certain crime and threatened and to perform an illegal operation by a criminal,” a static biometric authentication system may be “illegally operated, leading to heavy damage.” *Id.* at 1:19-24. The '228 Patent solved this problem by implementing a dynamic biometrics authentication system using communication between two devices in which a first device acquires dynamic biometric information in response to a static biometric authentication response from the second device, and the second device receives such information and displays information on a display screen based on a “mental state” of the user that is determined using the received dynamic biometric information. *See id.* at 1:9-1:21; 20:19-54 (Claim 1).

More specifically, the claimed invention is directed to a system comprising a first device, which performs a method of acquiring dynamic biometric information from a body of a user upon a second device performing static biometric authentication to verify a user and carry out an unlock operation, the first device then transmitting the acquired dynamic biometric information to the second device. *See id.* at 20:19-54 (Claim 1). For example, one embodiment discloses the second device as a mobile smartphone that performs static biometric authentication such as fingerprint authentication using a fingerprint sensor to unlock itself. *Id.* at 10:65, 13:20-31. The second device then performs communication with the first device,

requesting the first device to confirm the state of the authenticated user with dynamic biometric detection. *Id.* at 13:51-53.

Next, the first device then performs a method of determining the state of the authenticated user through detection of the user's dynamic biometric information. *Id.* at 13:54-58. Examples of a first device could be a wearable ring or wristwatch that measures dynamic biometric information such as temperature, blood pressure, and heart rate. *Id.* at 3:24-38, 4:36-46. In one embodiment, the first device receives dynamic biometric information through sensors measuring these biometrics, then transmits this dynamic biometric information to the second device. *Id.* at 14:45-50.

Finally, when the second device receives the dynamic biometric information from the first device, the second device performs a method of determining a "permission level" displaying specific information on the device's display screen based on the determined state of the authenticated user. *See id.* 14:10-44. In one embodiment, the second device compares the acquired dynamic biometric information with stored values in the authenticated user's "normal state" to determine whether the user is in a stress state. *See id.* at 13:56-14:2, 14:45-50. Based on the determined state of the user, specific application software may be restricted on the second device's display screen, as shown below in FIGS. 11A and 11B of the '228 Patent:

FIG. 11A

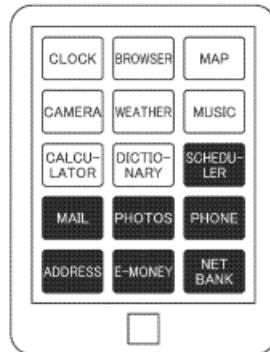
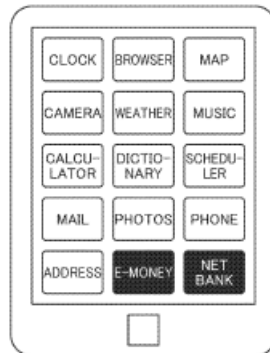


FIG. 11B



Id. at Figs. 11A-11B.

As a result, the user's access to application software through the display screen on the second device may be limited depending on the determined state of the authenticated user using the received dynamic biometric information acquired from the first device. Even in the case where static biometric information alone is sufficiently authenticated, therefore, access to application software may still be limited depending on the device's determined state of the user, based on the user's dynamic biometric information.

B. '228 Patent Prosecution History

U.S. Application No. 16/535,574 (the “‘574 Application”), which issued as the ‘228 Patent, was filed on 8/8/2019. EX1001, Cover Page. The ‘574 Application claimed priority to U.S. Application No. 15/315,735, filed June 12, 2014. *Id.* The examiner of the ‘574 Application rejected the claims on the basis of non-statutory double patenting in light of the application’s parent, U.S. Patent No. 10,423,769. EX1002, 353-56. This rejection was overcome through a terminal disclaimer. *Id.*, 328-29. The examiner then allowed the claims on the basis that the prior art of record did not disclose or render obvious the independent claims. *Id.*, 12-13.

C. Person Of Ordinary Skill In The Art

At the time of the ‘228 Patent, a POSITA would have a Bachelor of Science degree in Electrical Engineering, Computer Engineering, Computer Science, or a related technical field, with at least two years of experience working in the field of biometrics and smart, portable consumer electronics. Pet. at 7; *see also* EX1003, ¶46. More education (e.g., a Master’s degree) or relevant work experience may compensate for a deficit in one of the relevant qualifications stated above. *See* Pet. at 7; *see also* EX1003, ¶46.

For the purposes of this Preliminary Response, Patent Owner does not contest that the relevant fields of art include computer science and electrical or computer engineering with experience in biometric systems. While Patent Owner may not

agree with the precise level of experience proposed by Petitioner, these differences need not be resolved at this stage. Patent Owner reserves the right to provide further evidence and argument on this issue at a later time. The prior art cited by the Petitioner would have been understood by a POSITA under either definition.

D. Summary Of Petitioners' Proposed Grounds Of Unpatentability And The References Cited

The Petition raises six grounds of alleged obviousness based on the following five references:

Ground	'228 Patent Claim(s)	Type of Challenge	Primary Reference	Secondary Reference(s)
1	1-2, 4-7, 12-13, 15-18	§ 103	Aminzade	Sowers
2	1-2, 4-7, 12-13, 15-18	§ 103	Aminzade	Soli
3	3, 10-11, 14, 21-22	§ 103	Aminzade	(1) Sowers (2) Hong
4	3, 10-11, 14, 21-22	§ 103	Aminzade	(1) Soli (2) Hong
5	8-9, 19-20	§ 103	Aminzade	(1) Sowers (2) Altman
6	8-9, 19-20	§ 103	Aminzade	(1) Soli (2) Altman

1. Aminzade (EX1004)

Aminzade, titled "Mobile Computing Device and Wearable Computing Device Having Automatic Access Mode Control," was filed on October 2, 2013 and issued on March 10, 2015. EX1004, cover page.

Aminzade discloses a processing system including a mobile computing device configured with a wearable computing device, whereby the wearable computer device includes a sensor that outputs an indication that the wearable computer device is being worn. EX1004, Abstract, 8:34-53. The wearable computing device can be configured to communicate with the mobile computing device to perform functions such as changing user access to the mobile computing device from a reduced access mode to an increased access mode based on collected data such as the user's fingerprint. *Id.* at 8:34-53, FIG. 4.

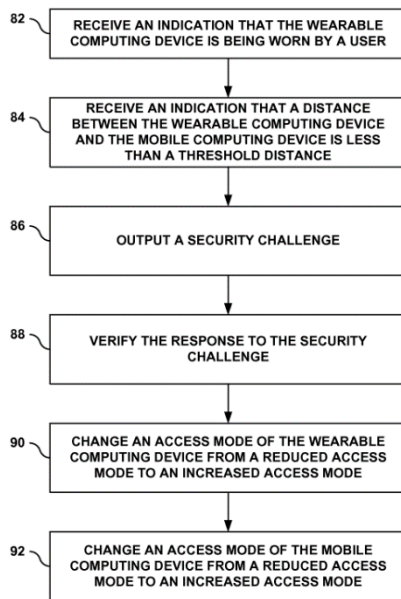


FIG. 4

EX1004 at FIG. 4.

Notably, the initial “reduced access” mode still allows user access to a “reduced set of functionality provided by the computing device.” *Id.* at Abstract, 8:34-53. Most importantly, Aminzade is completely silent as to any disclosure of

“lock,” “locking,” “unlock,” or “unlocking” operations, functions, and/or states. *See generally id.*

III. LEGAL STANDARD

A claim is not patentable if the differences between the claim and the prior art are such that the subject matter as a whole would have been obvious to a person of ordinary skill in the art at the time of the invention. 35 U.S.C. § 103(a). Obviousness requires assessing (1) the “level of ordinary skill in the pertinent art,” (2) the “scope and content of the prior art,” (3) the “differences between the prior art and the claims at issue,” and (4) “secondary considerations” of non-obviousness such as “commercial success, long felt but unsolved needs, failure of others, etc.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007) (quoting *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17-18 (1966)).

It is a petitioner’s burden “to demonstrate both ‘that a skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention, and that the skilled artisan would have had a reasonable expectation of success in doing so.’” *Intelligent Bio-Systems, Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1367-68 (Fed. Cir. 2016) (quotations and citations omitted). However, a petitioner must first show that all of the claimed elements are disclosed in the prior art. *See Medichem, S.A. v. Rolabo, S.L.*, 437 F.3d 1157, 1164

(Fed. Cir. 2006) (considering motivation to combine and reasonable expectation of success only “if all the elements of an invention are found in a combination of prior art references”).

IV. PETITIONER'S EXPERT DECLARATION IS ATTORNEY ARGUMENT PRESENTED IN THE CLOTH OF EXPERT TESTIMONY

Petitioner relies on a declaration from its expert Dr. Seth Nielsen (EX1003). However, Dr. Nielsen copies verbatim Petitioner's arguments and lacks sufficient facts and data to support his positions. For example:

Petition	Dr. Nielsen's Declaration (EX1003)
A POSITA also would have understood that this Aminzade functionality implicitly and inherently (necessarily) includes determining that the acquired static biometric information (e.g., a fingerprint) matches (an authentication result) the stored security challenge response. EX1003, ¶90 (Pet. at 33)	In my opinion, a POSITA also would have understood that this functionality of Aminzade implicitly and inherently (necessarily) includes determining that the acquired static biometric information (e.g., a fingerprint) matches (an authentication result) the stored security challenge response. (EX1003, ¶90)
It also would have been obvious to a POSITA to have telemetry module 28 and communication unit 64 receive the instruction from telemetry module 18 and communications units 44 as a matter of symmetry, and in light of Aminzade's disclosures that they are used for wireless communication between the two devices, described above. EX1003, ¶96 (Pet. at 39)	It also would have been obvious to a POSITA to have telemetry module 28 and communication unit 64 receive the instruction from telemetry module 18 and communications units 44 as a matter of symmetry, and in light of Aminzade's disclosures that they are used for wireless communication between the two devices, described above. (EX1003, ¶ 96)

Petition	Dr. Nielsen's Declaration (EX1003)
A POSITA would have understood that Aminzade implicitly and necessarily (inherently) discloses that communication unit 64 and telemetry module 28 perform communication of the instruction (which relat[es] to the authentication result) to access mode module 26 and processor 60 on which it executes, such as being communicated via channel 72. Otherwise, access mode module 26 and processor 60 could not give effect to the instruction, contrary to Aminzade's disclosure of increasing the access mode, described below. <i>See also</i> § IV.A ("performs communication" includes communication within a device); EX1003, ¶102 (Pet. at 41-42)	A POSITA would have understood that Aminzade implicitly and necessarily (inherently) discloses that communication unit 64 and telemetry module 28 perform communication of the instruction (which relat[es] to the authentication result) to access mode module 26 and processor 60 on which it executes, such as being communicated via channel 72. Otherwise, access mode module 26 and processor 60 could not give effect to the instruction, contrary to Aminzade's disclosure of increasing the access mode, described below. <i>See also</i> § IV.A ("performs communication" includes communication within a device). EX1003, ¶102
A POSITA would have understood that the disclosed "instruction" to the wearable device 20 to change its access mode "to an increased access mode" necessarily (inherently) results in the wearable device 20 changing its access mode accordingly (executes an unlock² operation to unlock itself in response to the communication relating to the authentication result). Otherwise, the instruction would have no effect. The unlock[ing] occurs in response to the wearable device 20 receiving the instruction (the communication relating	A POSITA would have understood that the disclosed "instruction" to the wearable device 20 to change its access mode "to an increased access mode" necessarily (inherently) results in the wearable device 20 changing its access mode accordingly (executes an unlock operation to unlock itself in response to the communication relating to the authentication result). Otherwise, the instruction would have no effect. The unlock[ing] occurs in response to the wearable device 20 receiving the instruction (the communication relating

² Both Petitioner and Dr. Nielsen (by nature of his regurgitation of Petitioner's arguments) misstate the content of Aminzade here. Namely, the word "unlock" is not mentioned anywhere in Aminzade. *See generally* EX1004.

Petition	Dr. Nielsen's Declaration (EX1003)
to the authentication result), as described above. EX1003, ¶106 (Pet. at 42-43)	to the authentication result), as described above. EX1003, ¶107

Dr. Nielsen does not provide any other analysis or explanation why a POSITA would find something obvious or be motivated to modify Aminzade other than Petitioner's own conclusory and boilerplate statements. The above citations are merely exemplary for Ground 1 (obviousness based on Aminzade alone) but Petitioner employs the same tactics for each of the other Grounds. *See generally* §§ VII.(B)-(F) *infra*.

Such conclusory and superficial attorney argument in the guise of expert testimony cannot serve as sufficient support for Petitioner's arguments. *See, e.g., Cardiacom, LLC v. Bosch Healthcare Sys., Inc.*, IPR2013-00439, Paper 26, 15-16 (P.T.A.B. Jan. 16, 2014); *see also Kinetic Techs., Inc. v. Skyworks Solutions, Inc.*, IPR2014-00529, Paper 8, 15-16 (P.T.A.B. Sept. 23, 2014) ("Merely repeating an argument from the Petition in the declaration of a proposed expert does not give that argument enhanced probative value," and a petitioner cannot move forward to trial based upon such "mere conclusory statements.") (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)); *TRW Auto. US LLC v. Magna Elecs., Inc.*, IPR2014- 00258, Paper 18, 10-11 (P.T.A.B. Aug. 27, 2014) (giving little to no weight to expert

testimony that “did not elaborate on [Petitioner’s] position because it simply repeated [Petitioner’s] conclusory statements verbatim”); *see also InfoBionic, Inc. v. Braemar Mfg., LLC*, IPR2015-01704, Paper 11, 6 (P.T.A.B. Feb. 16, 2016) (denying institution because expert merely repeated the argument in the Petition about what a reference meant without explaining why the expert believed that meaning to be correct).

Moreover, such conclusory opinions by an expert that merely parrot Petitioner’s arguments should be accorded little weight when used to supply a missing limitation. *See Xerox Corp. et al. v. Bytemark, Inc.*, IPR2022-00624, Paper 12, 5 (P.T.A.B. Feb. 10, 2023) (Former Director Vidal noting in a Sua Sponte affirmation of the decision: “I determine that the Board was correct in giving little weight to Petitioner’s expert because the expert declaration merely offered conclusory assertions without underlying factual support and repeated, verbatim, Petitioner’s conclusory arguments.”). Former Director Vidal stated that:

The declaration does not provide any technical detail, explanation, or statements supporting why the expert determines that the feature in question was required or would have been obvious based on the prior art disclosure. *See* Ex. 1003 ¶ 54. Instead, the declaration copies, word-for-word, Petitioner’s conclusory assertions. *Compare id.*, with Pet. 28–29. The declaration sets forth Petitioner’s conclusory assertions as though they are facts, rather than setting forth facts and evidence in

support of Petitioner's assertions. Accordingly, I agree with the Board's explanation that "the cited declaration testimony is conclusory and unsupported, adds little to the conclusory assertion for which it is offered to support, and is entitled to little weight" under 37 C.F.R. § 42.65(a).

Id. As discussed *infra*, Dr. Nielsen's "opinions" are copied verbatim from the Petition, including in attempting to fill in missing limitations.

Therefore, little to no weight should be given to Dr. Nielsen's testimony. And, absent his conclusory testimony, the Petition has no evidentiary support. Institution should be denied for this reason.

V. CLAIM CONSTRUCTION

In order to overcome the deficiencies of its primary reference, Aminzade, Petitioners advocate for a construction of "unlock operation" or "unlock" that is contrary to the plain and ordinary meaning of the term and the intrinsic record. *See* Pet. 9. In particular, Petitioners allege that the claimed "unlock operation" includes allowing the user to "access **additional** functionality on the device" from a limited access mode. *See id.* (arguing that steps S1003, S1007, and S1008 of FIG. 10 are included in the unlocking process). In essence, Petitioners are advocating that switching a device from one mode to another mode that offers additional functionality meets the claimed "unlock operation." Petitioners are forced to take

such an overly broad construction because Aminzade—the only reference Petitioners rely on to teach this limitation—is completely silent as to any “lock” or “unlock” operation. *See* EX1004.

Such an interpretation, however, is completely inconsistent with the intrinsic record.

The intrinsic record repeatedly discloses “unlock operation” consistent with its plain and ordinary meaning. For example, the '228 Patent discloses:

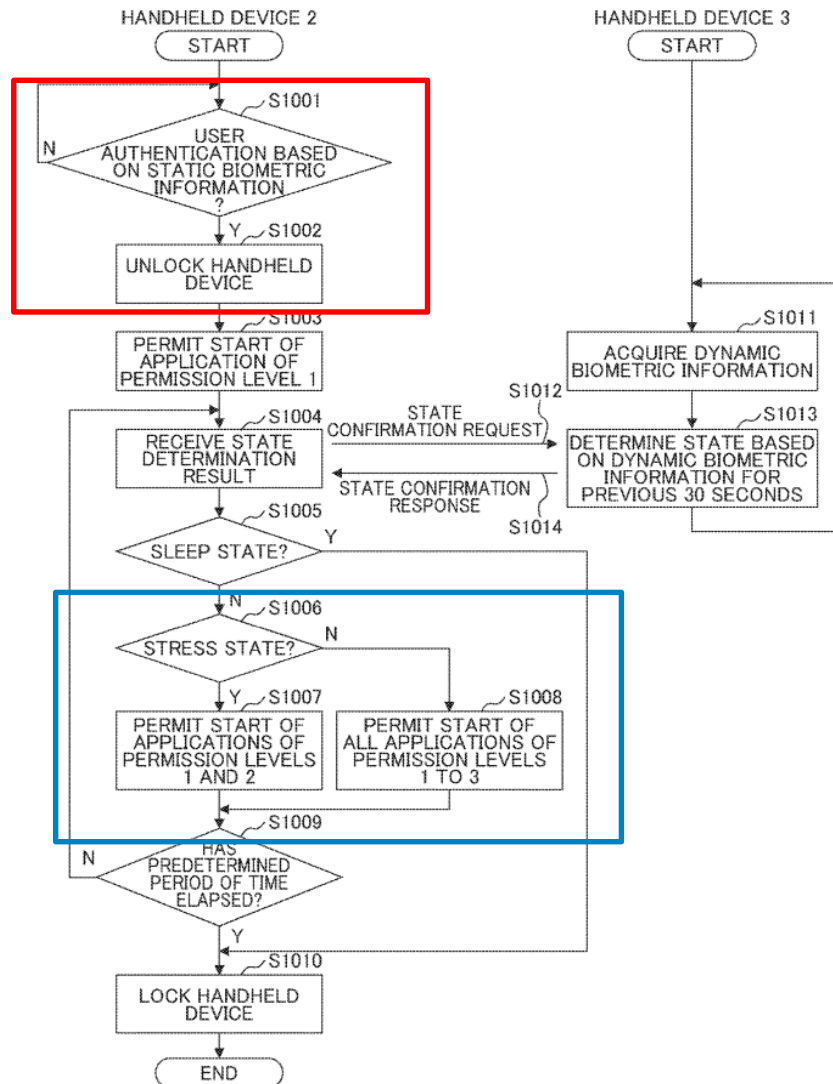
When the user is authenticated to be the authorized user, the lock control unit 1013 is controlled such that the handheld device 1 is **unlocked**.

The lock control unit 1013 is controlled by the **user authentication unit 1011** such that the lock control unit 1013 **unlocks the handheld device 1**, and, for example, when the user interface 1040 is not operated for a certain period of time, the lock control unit 1013 locks the handheld device 1. Further, even when the state determination unit 1012 is determined to be in a sleep state, the lock control unit 1013 locks the handheld device 1.

EX1001, 6:36-47 (emphasis added).

Thus, the '228 Patent describes an unlock operation that is carried out by the “lock control unit” in response to user authentication such that the handheld device is moved from a locked state to an unlocked state.. *See id.*; *see also id.* at 7:32-37, 8:53-59, 9:13-20, FIG. 10 (Step S1003).

Moreover, **after** an unlock operation, the '228 Patent distinguishes between lock and unlock state and switching modes to provide access to **additional** functionalities by describing the using of a “state determination unit” that carries state determination *after* the device is unlocked. EX1001 6:48-63 and Fig. 10. For example, the state determination unit determines a “permission level” of access above permission level 1 based on the state of the user and then provides access to additional functionalities at different permission levels, independent of the unlock operation that had already occurred at step S1002 through S1003. *Id.* For example, access to applications of permission levels 1 and 2 is provided at S1007 or S1008, which is related to determination of stress state. *Id.* at Fig. 10 (excerpted below with red box showing unlock operation and blue box showing access to additional functionalities).



EX1001 FIG. 10.

Extrinsic evidence also supports this plain and ordinary meaning of “an unlock operation” as evidenced by Samsung’s own documentation that describes unlock as an operation linked to providing access to the device after switching from a locked state, not simply providing access to additional functionalities. See EX2016

(<https://www.samsung.com/us/support/troubleshoot/TSG10001451/>) (excerpted

below); *see* *also* EX2017

(<https://www.samsung.com/us/support/answer/ANS10002881/>) (excepted below):

Unable to unlock Galaxy phone or tablet's screen

If your phone or tablet is not recognizing your PIN, pattern, password, fingerprint, or face unlock, rebooting the device or entering Safe Mode can help solve the problem. Sometimes you may be prompted to try an alternate method, like your password.

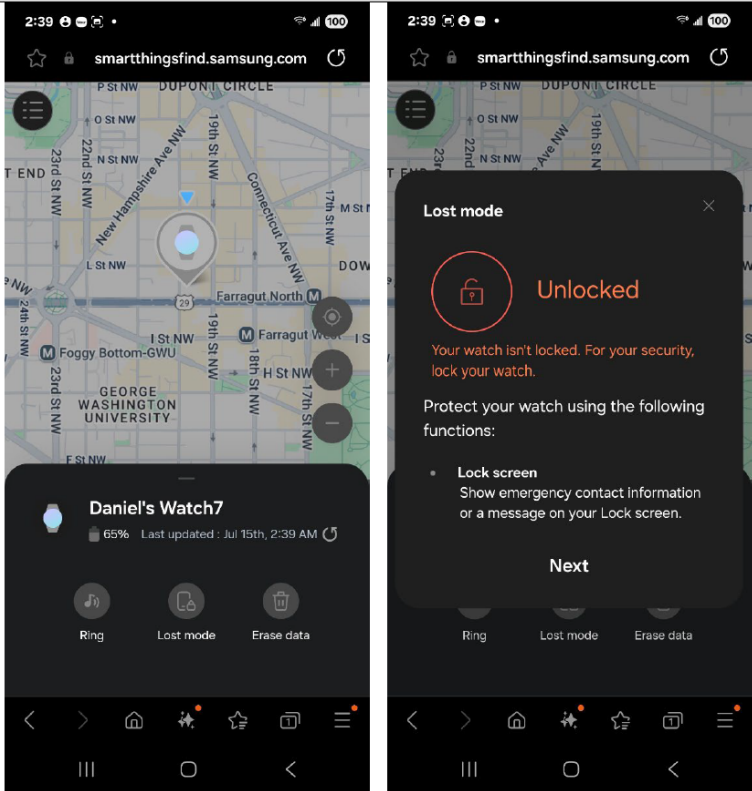
Lock and unlock Samsung DeX

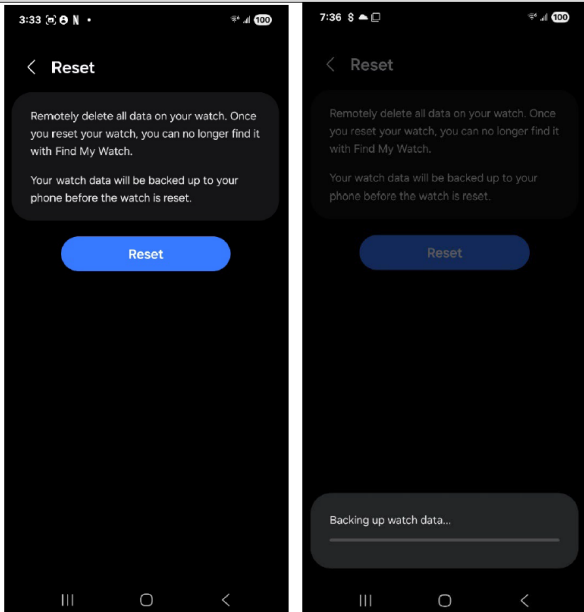
Locking and unlocking Samsung DeX is easy! You just need to select the Lock DeX option in the Samsung DeX screen on your connected device, such as your monitor. If you have Facial recognition or another type of Lock screen set up to get into your phone or tablet, for instance, you will need to use it to get back into DeX.



This is also consistent with Maxell's Infringement Contentions, where the infringement theories specifically identifies examples of unlocking operations, such as unlocking from lost state or unlocking by executing a reset operation. *See* EX1014 at 218, 223 (excerpted below):

Case IPR2025-01313
Patent No. 10,783,228
Patent Owner's Preliminary Response

U.S. Patent No. 10,783,228	Exemplary Evidence of Infringement
	

U.S. Patent No. 10,783,228	Exemplary Evidence of Infringement
	

Indeed, the Samsung device itself states “Unlocked”—to refer to the operation—which is in contrast to Aminzade that is completely silent as to the implementation of any “unlock” operation.

Additionally, Petitioner's expert Dr. Seth Nielsen's conclusory opinion does nothing to bolster Petitioner's proffered construction of this term. *See* EX1003 ¶¶ 52-53. Specifically, Dr. Nielsen cites to no dictionary or other evidence to support his opinion that his proffered definition is the plain and ordinary meaning of “unlock.” *See id.* Rather, Dr. Nielsen merely relies on the '228's functionality to “start applications with certain permission levels” (Steps S1007 and S1008), as a result of the S1002 unlock step, to argue a construction of “unlock” that includes “allowing the user to access additional functionality on the device.” *See id.* (citing EX10001, FIG. 10 (S1003, S1007, S1008)). Dr. Nielsen's conclusory statements are insufficient to bolster Petitioner's construction because they fail to “disclose [any] underlying facts or data on which the opinion is based[.]” *See id.*; Pet. 9; *InfoBionic, Inc. v. Braemar Manufacturing, LLC*, IPR2015-01704, Paper 11, at 14-15 (P.T.A.B. Feb. 16, 2016) (denying institution) (citing 37 C.F.R. § 42.65(a)) (“Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.”).

Moreover, Dr. Nielsen sets forth a definition of the term “unlock” that is inconsistent with his own use of the term in his patent U.S. Patent No. 8,745,379 (“the ‘379 Patent”). See EX2018. The ‘379 Patent, of which Dr. Nielsen is an inventor, sets forth an “**authentication process**,” which “may be advantageously employed to develop elegant single sign-on solutions, such as, **unlocking** a sensitive data vault.” *Id.* at 25:66-27:1. This definition is consistent with the plain and ordinary meaning of “unlock” as related to “authentication” for unlocking access as set forth above, not to providing “additional functionality,” like Dr. Nielsen proposes now. Compare *id.* (“authentication process . . . employed to . . . unlock[.]”), with EX1003 ¶ 53 (“the plain meaning of ‘unlock[ing]’ a device includes allowing the user to access additional functionality on the device.”).

Indeed, the ‘379 Patent states “unlocking” to refer to an operation carried out in response to an “authentication” operation, which is in contrast to Aminzade that is completely silent as to the implementation of any “unlock” operation.

VI. THE BOARD SHOULD DENY INSTITUTION IN VIEW OF SAMSUNG’S INDICATION THAT IT IS NOT LIMITED TO ASSERTING A DIFFERENT CLAIM CONSTRUCTION OF ANY CLAIM TERM FOR ANY OTHER PURPOSE

In its Petition, Samsung asserts:

Petitioner **does not contend that its proposed constructions are complete constructions** of these limitations or the claims **for any**

other purpose, including for issues that have been raised in the related litigation. . . . Any claim term not listed below should be construed according to its plain meaning to a POSITA at the time of the '228 patent's priority date.

Pet. 8. (emphasis added).

By refusing to contend that the proffered constructions here are “complete constructions[,]” Petitioner indicates that it will be taking different claim construction positions “for any other purpose, including for issues that have been raised in the related litigation.” *See id.* In view of Petitioners' broad *Sotera* stipulation, this “any other purpose” includes invalidity challenges Petitioner intends to present to the District Court based on the following system prior art:

h. '228 Patent

Prior Art Products and Systems – U.S. Patent No. 10,783,228	
• Samsung Galaxy S5, including model no. SM-G900, as described by the documents cited in Exhibit 228-4. • Samsung Gear 2, including model nos. SM-R380 and SM-R381, as described by the documents cited in Exhibit 228-5. • Discovery is ongoing, and Defendants will identify additional products and systems as they become available.	

EX2015, 34.

This “any other purpose” also includes allegations in District Court Proceeding that nearly every term in the '228 Patent's asserted claims is invalid under 35 U.S.C. § 112 for lack of written description. EX2015, 173-183.

g. '228 Patent

'228 Patent			
No.	Term	Claims	Reason
1	“a second communication interface that performs communication relating to the authentication result with the first	1	Lack of written description

Case IPR2025-01313
Patent No. 10,783,228
Patent Owner's Preliminary Response

'228 Patent			
	communication interface and receives the dynamic biometric information transmitted from the first communication interface"		
2	"[wherein the first information processing device ...] performs communication relating to the authentication result between the first communication interface and the second communication interface and executes an unlock operation to unlock itself in response to the communication relating to the authentication result"	1	Lack of written description
3	"[wherein the first information processing device ...] acquires the dynamic biometric information from the dynamic biometric information acquisition sensor after unlocking"	1	Lack of written description
4	"[wherein the first information processing device ...] maintains the unlocked state during a condition that the dynamic biometric information can be acquired"	1	Lack of written description
5	wherein the second information processing device receives the dynamic biometric information via communication between the first communication interface and the second communication interface and the display screen displays information based on a state of the user that is determined using the received dynamic biometric information	1	Lack of written description
6	"wherein the first information processing device continuously acquires the dynamic biometric information after being unlocked and the second information processing device receives the dynamic biometric information transmitted from the first communication device continuously or based on starting of an application on the second information processing device"	7	Lack of written description
7	"wherein the second information processing device gets position information denoting a position of the second information processing device and automatically transmits the position information to a predetermined address based on reception of a user input that is determined to be a predetermined type of user input during a	8	Lack of written description
'228 Patent			
	time period, wherein the predetermined address is not inputted by the user during the time period"		
8	"wherein the position information is automatically transmitted in response to the user input and without requiring additional user input that explicitly requires approval of the automatic transmission of the position information during the time period"	9	Lack of written description

Id. at 180-182.

Yet, here, Petitioner attests that these exact same terms are clear, require no construction, and are readily comparable to the prior art. *See* Pet. 8 ("Any claim term not listed below should be construed according to its plain meaning to a POSITA at the time of the '228 patent's priority date.").

Thus, by conceding that its proposed constructions here are not “complete constructions,” particularly in light of inconsistent constructions “in the related litigation,” Petitioner is indicating that it wants to have the flexibility to take different claim construction positions “for any other purpose” including even for additional invalidity arguments. Such reservation of rights does not comply with the requirements of 37 C.F.R. § 42.104(b)(3) and this Board’s prior decision.

Specifically, under 37 C.F.R. § 42.104(b)(3), petitioners must clearly articulate **in the petition** “[h]ow the challenged claim is to be construed.” If, according to Petitioner, its claim construction positions in this Petition are not “complete constructions,” then how does Petitioner propose that the Board construe such limitations to assess Petitioner’s invalidity challenges, particularly where such constructions would result in an inconsistent record with Petitioner’s proffered constructions in the District Court litigation. Petitioner is silent and provides no explanation for its basis for being non-committal in its position of claim construction to obtain an institution decision in this forum, only to turn around and seek a “different claim construction of any claim term for any other purpose” in District Court litigation. Indeed, Petitioner has done just that in prior IPRs where it argued for a plain and ordinary meaning of “character” in IPR2024-00735 and IPR2024-00777, but argued for a narrower construction of the same term in a jury trial to

argue for non-infringement. *See e.g.*, IPR2024-00735, Paper No. 38 at 9-10; *see also* IPR2024-000828, Paper No. 39 at 6-10 (contending in the IPR that “mode” should be given its plain and ordinary meaning but arguing in front of the jury that two modes require the implementation of two algorithms).

As established by this Board, a petitioner must explain why it takes different claim construction positions in the petition and in district court. *See Revvo Technologies, Inc. v. Cerebrum Sensor Technologies, Inc.*, IPR2025-00632, Paper 20 (Squires November 3, 2025) (precedential) (a petitioner must explain why it takes different claim construction positions in the petition and in district court); *American Airlines, Inc. et al v. Intellectual Ventures I LLC*, IPR2025-01055, Paper 11 (November 21, 2025) (denying institution when Petitioner was construing terms as plain and ordinary in the Petition, yet arguing for indefiniteness in a different forum). Thus, Petitioner's assertion of two different claim construction positions in the two forums alone favors denial of institution.

Instead of agreeing to be bound by the claim construction positions or lack thereof set forth in this Petition, Petitioner refuses to contend that the proffered constructions here are “complete constructions . . . for any other purpose, including for issues that have been raised in the related litigation[.]” The Board or Patent Owner should not be burdened with such an unbounded position on claim

construction when defending its patent rights. Indeed, this is the precise reason why 37 C.F.R. § 42.104(b)(3) requires Petitioner to explain how the challenged claims are to be construed. Petitioner cannot have it both ways.

Accordingly, for this reason alone the Board should deny institution of this petition.

VII. THE PETITION DOES NOT SHOW A REASONABLE LIKELIHOOD OF PREVAILING WITH RESPECT TO ANY CHALLENGED CLAIM

In addition to the grounds already presented in Patent Owner's Request for Discretionary Denial, institution should be denied because Petitioners do not establish a reasonable likelihood of prevailing against any challenged claim.

A. Ground 1: Petitioners Fail To Establish That Claims 1-2, 4-7, 12-13, and 15-18 are Rendered Obvious By Aminzade in View of Sowers

Petitioners have not shown a likelihood of prevailing with respect to Ground 1 because Aminzade in view of Sowers does not teach each and every element of Claims 1-2, 4-7, 12-13, and 15-18. Specifically, Aminzade in combination with Sowers does not teach elements [1.c], [1.d], [1.e] (and comparable elements of claim 12: [12.f], [12.g], [12.h]), as required for each of these claims. Additionally, because dependent claims 2, 4-7, 13, and 15-18 depend from independent claims 1 and 12 that Petitioners have not shown to be unpatentable, Petitioners have also failed to

show that claims 2, 4-7, 13, and 15-18 are unpatentable by Aminzade in view of Sowers.

1. No Motivation to Combine Aminzade with Sowers

Petitioners have not shown how a POSITA would have combined the teachings of Aminzade with the teachings of Sowers with any expectation of success. Sowers is not analogous to Aminzade or the '228 Patent because they are in different fields of invention and do not seek to solve the same pertinent particular problem. Moreover, Petitioners and their expert fail to articulate any rationale as to why a POSITA would combine the mobile device authentication system of Aminzade with the dynamic biometric monitoring of Sowers.

Analogousness requires prior art to be in the “same field of endeavor” or “reasonably pertinent” to a similar problem being solved by the claimed invention. *In re Klein*, 647 F.3d 1343, 1348 (Fed. Cir. 2011) (citation omitted). The '228 Patent is directed to the field of “biometrics authentication,” to detect and prevent a situation where authentication may be carried out against a “user’s will” and a device may be “illegally operat[ed].” See EX1001, Summary of the Invention. In other words, the '228 Patent is directed towards enhancing security of a mobile device through an authentication system that limits access in situations where a user may be coerced to access the mobile device. See *id.*

A POSITA would not be motivated to combine Aminzade with Sowers because Sowers is in a different field of endeavor than both the '228 Patent and Aminzade. Petitioners argue that because Sowers and Aminzade are both wearable devices with sensors and continuous wireless communication with mobile devices containing applications, they are compatible systems with sufficient similarities that a POSITA would have been motivated to combine the two. *See* Pet. 55-60. However, Sowers exists in a different field of endeavor from both the '228 Patent and Aminzade. On one hand, Aminzade is directed to limiting or increasing user access to mobile device functionality based on user location and detection of the wearable device being worn to “increase security” of the mobile device. EX1004, Summary, 9:35-40, 23:28-34, 25:50-58. On the other hand, Sowers discloses a wearable device for “health monitoring,” and only mentions security in the context of ensuring that acquired health data is HIPAA compliant. EX1005, Abstract, ¶¶21, 29. Unlike Aminzade, Sowers does not disclose altering security access to a mobile device’s applications or functionality. *See generally id.* Rather, Sowers exists in a wholly different field of endeavor because Sowers is directed to health monitoring and teaches security only in the context of ensuring collected healthcare data is HIPAA compliant. *See id.* at Abstract, ¶¶21, 29. Thus, Petitioners’ proposed combination of

Sowers and Aminzade fails the first test for analogousness because Sowers exists in a separate field of endeavor from both Aminzade and the '228 Patent.

Further, a POSITA wouldn't be motivated to combine Aminzade with Sowers because Sowers solves different pertinent problems than both Aminzade and the '228 Patent, failing the second test for analogousness. *See In re Klein*, 647 F.3d 1343, 1348 (Fed. Cir. 2011) ("A reference is reasonably pertinent if, even though it may be in a different field [of endeavor]. . . it is one which . . . logically would have commended itself to an inventor's attention in considering his problem.") (citation omitted). The '228 Patent's disclosed purpose is to detect and prevent a situation where authentication may be carried out against a "user's will" or "intension." *See* EX1001, Summary of the Invention. Additionally, Aminzade discloses limiting or increasing user access to mobile device functionality based on user location and detection of the wearable device being worn, for the disclosed purpose of "increas[ing] security" to the mobile device functionality. EX1004, Summary, 9:35-40, 23:28-34, 25:50-58. In contrast, Sowers is directed towards solving the issue of healthcare data privacy in health monitoring systems. Petitioners argue that a POSITA would be motivated to combine Sowers and Aminzade because Sowers teaches "limiting access to a user's health data" acquired by the wearable device "for HIPAA compliance." Pet. 58; *see* EX1005 ¶¶21, 29. Specifically, Petitioners argue

that Aminzade is related to the purpose of “seek[ing] increased security for the user’s health data” because it discloses heightened security measures that limit user access to “both devices if the user is no longer wearing the wearable device or is too far away.” Pet. 58; *see* EX1004 9:40-47. However, Aminzade does not mention anything about limiting access to the biometric data acquired for user authorization, nor is it directed to ensuring healthcare privacy standards of the biometric data storage in general. *See* EX1005 ¶¶21, 29. *See generally* EX1001, EX1004. Aminzade discloses **acquiring biometric information for the purpose of limiting access to a mobile device’s applications and functionality**, and is distinct from Sowers’s teaching directed **to limiting access to the acquired biometric information for healthcare confidentiality purposes**. *Compare* EX1004, Summary, 9:35-40, 23:28-34, 25:50-58 (disclosing purpose of “increas[ing] security” to mobile device functionality), *with* EX1001, Summary of the Invention (disclosing purpose to prevent a situation where authentication is carried out against a “user’s will” or “intension.”), *and* EX1005 ¶¶21, 28 (teaching communication and storage of health information “with security levels consistent with [HIPAA] requirements.”). Thus, Aminzade and the ’228 Patent are directed towards solving different pertinent problems than Sowers, failing the second test of analogousness.

Moreover, Petitioners and their expert fail to articulate any rationale as to why a POSITA would combine the mobile device authentication system of Aminzade with the dynamic biometric monitoring of Sowers. Petitioners simply provide conclusory statements that Sowers's disclosed "desirability to continuously monitor a user's health and provide notice of potential health problems" and "low cost, comprehensive, continuous monitoring of health information" would have motivated a POSITA to add Sowers's function to Aminzade merely because "Aminzade does not disclose such functionality" or "benefit." *See* Pet. 58-59; EX1005 ¶¶5, 7. Petitioners also argues that, according to Petitioners' expert Dr. Nielsen, implementing Sowers's functionalities in Aminzade's system would have been a "known and natural choice" because Aminzade is silent as to a specific application. Pet. 59; EX1003, ¶163. Petitioners' conclusory statements are insufficient and provide no factual support. *See* Pet. 58-60; *In re Nuvasive, Inc.*, 842 F.3d 1376, 1383 (Fed. Cir. 2016) (conclusory statements are "insufficient articulations of motivation to combine" references). Dr. Nielsen's expert statements do nothing to cure this deficiency, as Petitioners fail to "disclose [any] underlying facts or data on which the opinion is based[.]" *See* Pet. 59; EX1003, ¶163; *InfoBionic, Inc. v. Braemar Manufacturing, LLC*, IPR2015-01704, Paper 11, at 14-15 (P.T.A.B. Feb. 16, 2016) (denying institution) (citing 37 C.F.R. § 42.65(a))

(“Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.”). Thus, Petitioners and their expert fail to articulate any rationale rooted in fact or data as to why a POSITA would combine the mobile device authentication system of Aminzade with the dynamic biometric monitoring of Sowers.

Therefore, a POSITA seeking to solve the problem addressed by the '228 Patent, preventing unauthorized use of a mobile device through coerced user access, would not have been motivated to combine Aminzade and Sowers to arrive at the claimed invention. Sowers is non-analogous art because the reference is in a separate field of endeavor and does not address the pertinent particular problems solved by the '228 Patent or Aminzade. **Sowers teaches security measures directed to biometric data confidentiality in health monitoring systems, while Aminzade teaches the use of biometric data to enhance security of mobile device functionality.** Compare EX1004, Summary, 9:35-40, 23:28-34, 25:50-58, with EX1005 ¶¶21, 28. Combining these disparate teachings would not have logically led a POSITA to the claimed invention, particularly in the absence of any articulated rationale by Petitioners or their expert. As detailed below, such a combination still fails to disclose or suggest the key limitations of the challenged claims.

Therefore, a POSITA would not have been motivated to combine Aminzade with Sowers.

2. The Combination of Aminzade and Sowers Fails to Disclose Limitation [1.c] and [12.f]

Even when combined, Petitioners fail to show that Aminzade in combination with Sowers discloses claim elements [1.c] and [12.f]: “[a] first information processing device: perform[ing] communication relating to the authentication result between the first communication interface and the second communication interface and execut[ing] an unlock operation to unlock itself in response to the communication relating to the authentication result.” Specifically, neither Aminzade nor Sowers discloses the execution of “an unlock operation to unlock itself.” *See* EX1001 20:41-43 (Claim [1.c]), 22:6-8 (Claim [12.f]).

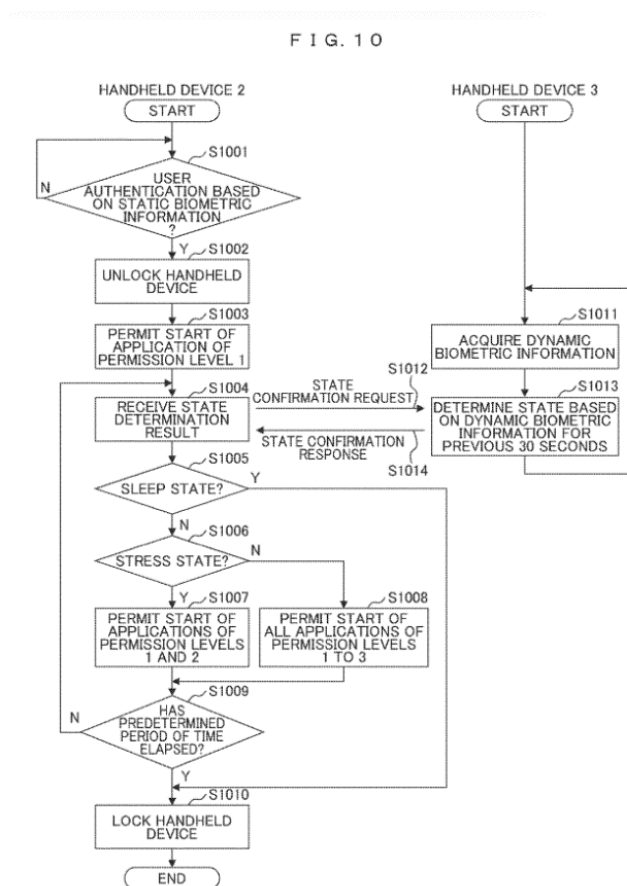
Petitioners rely on Aminzade to argue disclosure of an “unlock operation.” *See* Pet. 42-44, 53. However, the gap between Aminzade and the claims of the ’228 Patent is apparent under Petitioners’ proposed constructions of the claim term “unlock.” Petitioners argue that the plain meaning of “unlock[ing]” a device includes allowing the user to “access additional functionality on the device” from a reduced access mode. *See* Pet. at 9. As explained above, this construction is inconsistent with the ’228 Patent’s specification because it is overbroad in the context of the specification and conflates the ’228 Patent’s discrete unlock and state

determination functions carried out by the “lock control unit” and “state determination unit,” respectively. *See* § V.

In fact, Aminzade does not even disclose an unlocking operation. The Petition tacitly admits this by arguing for a construction of “unlock operation” that is not consistent with the plain and ordinary meaning. *See* Pet. at 9. That is why Petitioners rely on an incorrect construction of the term “unlock” to argue that Aminzade discloses an “unlock operation” in switching from a “reduced access mode” to an “increased access mode,” wherein “reduced access” is defined as user access to a “reduced set of functionality provided by the computing device.” *See id.* at 42-44; EX1004, Abstract, 1:38-45, 3:32-35, FIG. 4. Accordingly, applying the claim constructions offered herein, this functionality does not disclose an “unlock operation to unlock itself.” *See* § V.

A POSITA would understand that, in the context of the '228 specification, an unlock operation unlocks a device to an initial access mode from a locked state instead of switching to an “increased access mode” from a “reduced access mode.” *See* § V; EX1001 6:32-39, 7:15-21, 8:27-30, 7:47-49, 10:26-28, 13:28-31, FIG. 10. Further, a POSITA would understand that the '228 Patent's state determination unit analyzes user information of an already authenticated user to determine a “permission level” of access above permission level 1 *after* the handheld device is

unlocked to an initial permission level 1. *See* EX1001 FIG. 10 (depicting the unlock function in Steps S1002 and S1003, separate from the state determination function in Steps S1007 and S1008). The '228 Patent specification demonstrates that these two processes are distinct in its description that the permission level determination process carried out by the “state determination unit” may end if the user is determined to be in a sleep state, causing the handheld device to revert to a “locked” state,” described as “permission level 0.” *Id.* 8:26-30. The '228 specification mentions user access to “startable” applications in the context of permission levels 1, 2, and 3, not in the context of switching from locked state to unlocked state. *See id.* 7:32-37, 8:53-59, 9:13-20.



Id. at FIG. 10.

When this principle is applied to claim elements [1.c] and [12.f], specifically Aminzade's functionality of switching from a "reduced access mode" to "increased access mode," Aminzade does not disclose an "unlock operation to unlock itself" because Aminzade merely discloses switching modes from "reduced access mode" to "increased access mode" and never refers to these modes as locked versus unlocked states. In contrast, the challenged claims and the '228 Patent specifically recite an "unlock operation." See *id.* 7:32-37, 8:53-59, 9:13-20, FIG. 10 (Steps

S1002 and S1003). In Aminzade's "reduced access mode," the user has been authenticated and has access to a "reduced set of functionality" and there is no disclosures of this mode being a "locked" mode. EX1004, Abstract, 1:38-45, 3:32-35. As explained above and shown below in FIG. 10, this state determination process (Steps S1007 and 1008) is a discrete process from the '228 Patent's unlock function (Steps S1002 and S1003). See EX1001, FIG. 10. **Because Aminzade does not disclose an "unlock operation," as claimed, and only discloses switching reduced and increased functionality modes, Aminzade cannot be characterized as disclosing an "unlock operation to unlock itself[.]"**

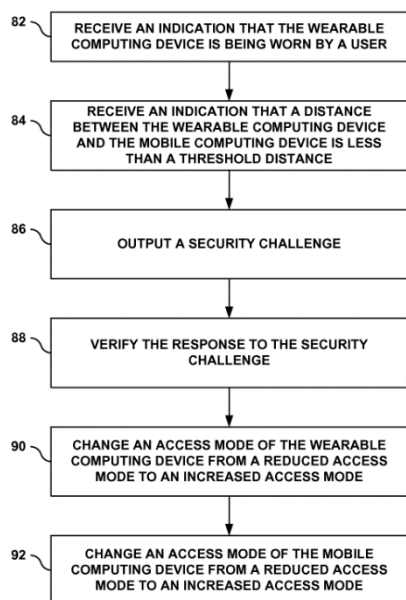
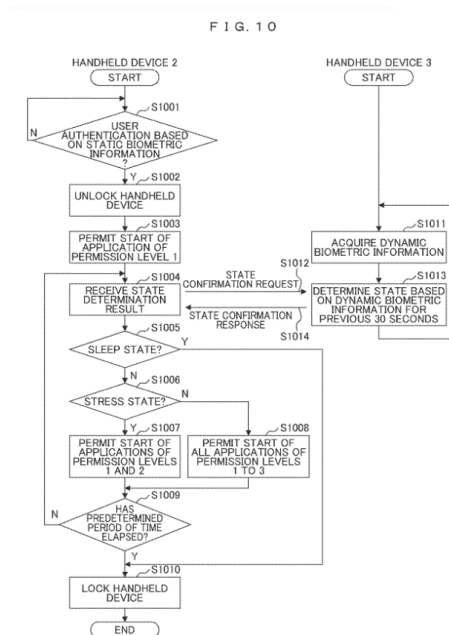


FIG. 4



EX1004 at FIG. 4; EX1001 at FIG. 10.

Abiding with the plain requirements of the claims, the unlock operation of claim limitations [1.c] and [12.f] cannot be considered to include determination of user access from a “reduced access mode” to an “increased access mode.” Thus, Aminzade does not disclose or define an “unlock operation to unlock itself.”

For these reasons, there is no reasonable likelihood of success of any claim challenged in Ground 1 because Petitioners have not shown that Aminzade in view of Sowers discloses claim elements [1.c] and [12.f].

3. The Combination of Aminzade and Sowers Fails to Disclose Limitation [1.d] and [12.g]

Petitioners fail to show that Aminzade in combination with Sowers discloses claim element [1.d] and [12.g]: “the [first information processing device] acquires the dynamic biometric information from the dynamic biometric acquisition sensor after unlocking[.]” Specifically, Petitioners fail to show that either reference discloses “unlocking.” Even when combined, neither Aminzade nor Sowers discloses an “unlocking” operation that triggers any condition because neither reference discloses an unlocking operation, as explained above. *See* § VII.A.2.

Additionally, Petitioners rely solely on Aminzade to argue a disclosure of an “unlocking” mechanism, and argue that Sowers’ disclosure of the remaining limitation (*acquir[ing] the dynamic biometric information from the dynamic biometric information sensor*) would have been obvious to include “after” the

“unlocking” mechanism. *See* Pet. 45-46, 53. As explained above, Aminzade does not disclose an unlocking mechanism. *See* § VII.A.2. Even if it did, Sowers discloses a **single** device to obtain multiple dynamic biometric information such as oxygen saturation of a person's blood and ECG/EKG. EX1005 ¶¶3-4. Sowers fails to disclose a lock/unlock mechanism between two devices because Sowers is an invention directed to “a single device” or “a single apparatus” to measure dynamic biometric information. *See id.* at ¶¶5-6. Thus, a lock/unlock mechanism is entirely out of the scope of Sowers. Additionally, the '228 patent sets forth the necessity to include dynamic biometric information (“emotional biometrics”) in its unlock operation out of consideration of “a situation in which the user is threatened and forced to perform an illegal operation by a criminal[.]” EX1001 1:54-59. However, Sowers does not take into account such a situation at all. *See* EX1005 ¶¶3-4 (mentioning situations where a “user's health information reflects a dangerous condition” only in the context of “industry standards of health.”). For this and other reasons set forth above, Petitioner's attempt to relate an lock/unlock operation to the acquisition of dynamic biometric information through combination of Aminzade with Sowers is mere impermissible hindsight. *See* § VII.A.1. Thus, a POSITA would not be motivated to combine Aminzade and Sowers to **acquire dynamic biometric information** after **unlocking**.

Therefore, Petitioners failed to establish a reasonable likelihood of success of any claim challenged in Ground 1.

4. The Combination of Aminzade and Sowers Fails to Disclose Limitation [1.e] and [12.h]

Petitioners fail to show that Aminzade in combination with Sowers discloses claim element [1.e] and [12.h]: “[the first information processing device] maintains the unlocked state during a condition that the dynamic biometric information can be acquired[.]” Specifically, Petitioners fail to show that either reference discloses “maintain[ing] the unlocked state” during any condition. Even when combined, neither Aminzade nor Sowers discloses an unlocking operation that causes an “unlocked state.” Moreover, even if Petitioners can successfully argue that Aminzade discloses an “unlocked state,” Aminzade does not disclose “maintain[ing]” such a state based on “a condition that the dynamic biometric information can be acquired.”

Aminzade does not disclose an “unlocked state” because, as explained above, Petitioners cannot show that Aminzade discloses an unlocking operation, and thus an “unlocked state,” according to the plain and ordinary meaning of the ’228 Patent’s specification. *See* § V.

Additionally, even if Petitioners could show that Aminzade discloses an “unlocked state,” it cannot be shown that such a state is “maintain[ed] during a

condition that the dynamic biometric information can be acquired” within the plain and ordinary meaning of the ’228 Patent specification. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1321 (Fed. Cir. 2005) (emphasizing that “the specification is the single best guide to the meaning of a disputed term.”) (internal quotations omitted). The ’228 Patent specification discloses that, depending on a condition, the first information processing device can either revert to a locked state or maintain an unlocked state within one of the permission levels. EX1001, 7:15-21, 8:27-30, 8:38-43.

Petitioners argue that Aminzade’s functionality of “remaining in increased access mode” discloses “maintain[ing] the unlocked state.” Pet. 46. However, Aminzade’s “reduced access mode” is the only alternative state to the increased access mode, wherein “reduced access” is defined as user access to a “reduced set of functionality provided by the computing device.” *See* EX1004, Abstract, 1:38-45, 3:32-35, 3:39-46, FIG. 4. Aminzade does not disclose any state other than an “increased access” and “reduced access,” neither of which can be considered “locked states” in the context of the ’228 Patent specification because both states disclose user access to startable applications. *Compare id.*, with EX1001 7:32-37, 8:53-59, 9:13-20 (mentioning startable applications only in the context of permission levels 1-3 after unlocking). Therefore, Aminzade does not disclose the functionality of

“maintain[ing] an unlocked state during a condition” because it does not operate to prevent the occurrence of a locked state under any condition. Rather, Aminzade only discloses two states, neither of which can be considered locked states in the context of the '228 specification.

Further, Petitioners rely solely on Aminzade to argue prior disclosure of “[a device] maintain[ing] the unlocked state during a condition,” and argue that Sowers’ disclosure of the remaining limitation (acquiring dynamic information) would have been obvious to include as such a condition. *See* Pet. 46-47, 53. Even if it could be found that Aminzade’s reduced access mode is equivalent to the “locked state” of the '228 Patent, and thus Aminzade discloses “maintain[ing] the unlocked state,” the reference still fails to disclose **“a condition that the dynamic biometric information can be acquired.”** *See* EX1004 16:59-17:9, 26:61-65 (disclosing no sensors for acquiring dynamic biometric information within the meaning of the '228 Patent). This deficiency is not recovered by the teachings of secondary prior art such as Sowers and Soli.

For example, Sowers discloses a single device to obtain multiple dynamic biometric information such as oxygen saturation of a person’s blood and ECG/EKG. EX1005 ¶¶3-4. However, Sowers fails to disclose a lock/unlock mechanism between two devices because Sowers is an invention directed to “a single device” or “a single

apparatus” to measure dynamic biometric information. *See id.* at ¶¶5-6. Thus, a lock/unlock mechanism is entirely out of scope of Sowers. Additionally, the '228 patent sets forth the necessity to include dynamic biometric information (“emotional biometrics”) in its unlock operation out of consideration of “a situation in which the user is threatened and forced to perform an illegal operation by a criminal[.]” EX1001 1:54-59. However, Sowers does not take into account such a situation at all. *See* EX1005 ¶¶3-4 (mentioning situations where a “user’s health information reflects a dangerous condition” only in the context of “industry standards of health.”). For this and other reasons set forth above, Petitioner’s attempt to relate an lock/unlock operation to the acquisition of dynamic biometric information through combination of Aminzade with Sowers is mere impermissible hindsight. *See* § VII.A.1.

As explained above, Aminzade does not disclose an “an unlocked state” because it does not disclose an unlock function or operation. *See* § VII.A.2. Even if Aminzade can be found to disclose “maintain[ing] the unlocked state” so as to prevent the occurrence of a locked state, it does not disclose “a condition that the dynamic biometric information can be acquired.” Additionally, a POSITA would not be motivated to combine Aminzade and Sowers to “maintain an unlocked state during a condition that dynamic biometric information can be acquired” for the reasons set forth above. *See* § VII.A.1.

Therefore, Petitioners fail to establish a reasonable likelihood of success of any claim challenged in Ground 1.

5. The Combination of Aminzade and Sowers Fails to Disclose Claims 7 and 18

Claims 7 and 18 recite: “the first [information processing] device continuously acquir[ing] dynamic biometric information after being unlocked and the second [information processing] device receiv[ing] the dynamic biometric information transmitted from the first communication device continuously or based on starting of an application on the [second information processing] device.”

Because claim 7 depends from Claim 1, and claim 18 depends from claim 12, both claims include all the limitations that Aminzade in combination with Sowers fail to teach, as detailed *supra* § VII.A.2-4 (claim limitations [1.c], [1.d], [1.e], [12.f], [12.g], [12.h]). Petitioners' argument for claims 7 and 18 fails for at least these same reasons.

Specifically, Petitioners cite back to their arguments for claim limitation [1.d] to argue that Aminzade combined with Sowers discloses “the first information processing device ‘continuous[ly]’ acquir[ing] the dynamic biometric information after being unlocked. See Pet. 51-52, 55. As set forth above, Aminzade does not disclose an “unlocking” operation, and a POSITA would not be motivated to combine Aminzade and Sowers to continuously acquire dynamic biometric

information after unlocking because Aminzade and Sowers are not analogous art and solve different pertinent problems. *See* §§ VII.A.1, VII.A.2.

For at least the foregoing reasons, Petitioners fail to show a reasonable likelihood of success in establishing that claims 7 and 18 would have been rendered obvious in view of Aminzade in combination with Sowers.

B. Ground 2: Petitioners Fail To Establish That Claims 1-2, 4-7, 12-13, and 15-18 are Rendered Obvious By Aminzade in View of Soli

Petitioners have not shown a likelihood of prevailing with respect to Ground 1 because Aminzade in view of Soli does not teach each and every element of Claims 1-2, 4-7, 12-13, and 15-18. Specifically, Aminzade in combination with Soli does not teach elements [1.c], [1.d], [1.e] (and comparable elements of claim 12: [12.f], [12.g], [12.h]), as required for each of these claims. Additionally, because dependent claims 2, 4-7, 13, and 15-18 depend from independent claims 1 and 12 that Petitioners have not shown to be unpatentable, Petitioners have also failed to show that claims 2, 4-7, 13, and 15-18 are unpatentable by Aminzade in view of Soli.

1. No Motivation to Combine Aminzade with Soli

Petitioners have not shown how a POSITA would have combined the teachings of Aminzade with the teachings of Soli with any expectation of success. Soli is not analogous to Aminzade or the '228 Patent because they are each in different fields of invention and do not seek to solve the same pertinent particular

problem. Moreover, Petitioners and their expert fail to articulate any rationale as to why a POSITA would combine the mobile device authentication system of Aminzade with the dynamic biometric monitoring of Soli.

Analogousness requires prior art to be in the “same field of endeavor” or “reasonably pertinent” to a similar problem being solved by the claimed invention. *In re Klein*, 647 F.3d 1343, 1348 (Fed. Cir. 2011) (citation omitted). The '228 Patent is directed to the field of “biometrics authentication,” to detect and prevent a situation where authentication may be carried out against a “user’s will” and a device may be “illegally operat[ed].” See EX1001, Summary of the Invention. In other words, the '228 Patent is directed towards enhancing security of a mobile device through an authentication system that limits access in situations where a user may be coerced to access the mobile device. See *id.*

A POSITA wouldn't be motivated to combine Aminzade with Soli because Soli is in a different field of endeavor than both the '228 Patent and Aminzade. Petitioners argue that because Soli and Aminzade are both wearable devices with sensors and wirelessly communicate with mobile devices, they are compatible systems with sufficient similarities that a POSITA would have been motivated to combine the two. See Pet. 81-82. However, Soli exists in a different field of endeavor from both the '228 Patent and Aminzade. On one hand, Aminzade discloses limiting

or increasing user access to mobile device functionality based on user location and detection of the wearable device being worn. EX1004, Summary, 9:35-40, 23:28-34, 25:50-58. Additionally, the '228 Patent is directed to the field of "biometrics authentication," and teaches an authentication system that limits access to a mobile device in situations where a user may be coerced to access the mobile device. *See* EX1001, Summary of the Invention. On the other hand, Soli discloses a wearable device to "aggregate[e] and shar[e] wellness data," and only mentions user authorization in the context of user access to the wellness data. *See* EX1006, ¶¶2, 7; EX1007, ¶¶2, 7. Soli does not disclose security functions that alter access to a mobile device's applications or functionality. *See generally* EX1006; EX1007. Rather, Soli exists in a wholly different field of endeavor from both Aminzade and the '228 Patent because Soli is directed to health monitoring. *See* EX1006, ¶7; EX1007, ¶7. Thus, Petitioners' proposed combination of Soli and Aminzade fails the first test for analogousness because Soli exists in a separate field of endeavor from both Aminzade and the '228 Patent.

Further, a POSITA wouldn't be motivated to combine Aminzade with Soli because Soli solves different pertinent problems than both Aminzade and the '228 Patent, failing the second test for analogousness. *See In re Klein*, 647 F.3d 1343, 1348 (Fed. Cir. 2011) ("A reference is reasonably pertinent if, even though it may

be in a different field [of endeavor]. . . it is one which . . . logically would have commended itself to an inventor's attention in considering his problem.") (citation omitted). The '228 Patent's disclosed purpose is to detect and prevent a situation where authentication may be carried out against a "user's will" or "intension" through the use of biometric data. *See* EX1001, Summary of the Invention. Additionally, Aminzade discloses limiting or increasing user access to mobile device functionality based on user location and detection of the wearable device being worn, for the disclosed purpose of "increas[ing] security" of the mobile device functionality. EX1004, Summary, 9:35-40, 23:28-34, 25:50-58. In contrast, Soli teaches secure healthcare data transfer and storage in health monitoring systems to maintain privacy of the acquired biometric data, which solves a different pertinent problem than both Aminzade and the '228 Patent. *See* EX1006, Abstract, ¶¶68, 225, 233-234, 469; EX1007, ¶¶40, 140, 148-149, 165, 384. Petitioners argue that a POSITA would be motivated to combine Soli and Aminzade because Soli teaches "transmitting wellness data to the user authorized to access the set of wellness data." Pet. 82; *see* EX1006, Abstract, ¶7; EX1007, ¶7. Specifically, Petitioners argue that this teaching would have motivated a POSITA to transmit the dynamic biometric data from Soli wearable device to Aminzade's mobile device, which authorizes the user to use the mobile device at a specific level of functionality via fingerprint

authentication. Pet. 82; *see* EX1004 9:40-47. However, Soli teaches authorization specifically for the purpose of “secure[]” storage and “transfer” of the acquired biometric data for data privacy purposes. *See* EX1006, Abstract, ¶¶68, 225, 233-234, 469; EX1007, ¶¶40, 140, 148-149, 165, 384. Aminzade does not mention anything about limiting user access to the biometric data acquired for user authorization and is not directed to secure transfer of the biometric data itself. *See generally* EX1004. Aminzade discloses **acquiring biometric information for the purpose of limiting access to a mobile device’s applications and functionality**, and is distinct from Soli’s teaching directed **to secure storage and transfer of the acquired biometric information for data privacy purposes**. *Compare* EX1004, Summary, 9:35-40, 23:28-34, 25:50-58 (disclosing purpose of “increas[ing] security” to mobile device functionality), *with* EX1006, Abstract, ¶¶68, 225, 233-234, 469 (teaching “secure[]” storage and “transfer” of biometric data for data privacy purposes), *and* EX1007, ¶¶40, 140, 148-149, 165, 384. Thus, Aminzade is directed towards solving different pertinent problems than Soli, failing the second test of analogousness.

Moreover, Petitioners and their expert fail to articulate any rationale as to why a POSITA would combine the mobile device authentication system of Aminzade with the dynamic biometric monitoring of Soli. Petitioners simply provide conclusory statements that Soli’s disclosed “desirability for users to ‘monitor and

track their wellness data” would have motivated a POSITA to add Soli’s function to Aminzade because “Aminzade does not elaborate on any specific application on its wearable device.” *See* Pet. 82-83; EX1006 ¶3; EX1007 ¶3. Petitioners also argue that, according to Petitioners’ expert Dr. Nielsen, implementing Soli’s functionalities in Aminzade’s system would have been a “known and natural choice” because Aminzade is silent as to a specific application. Pet. 82-83; EX1003, ¶249. Petitioners’ conclusory statements are insufficient and provide no factual support. *See* Pet. 81-83; *In re Nuvasive, Inc.*, 842 F.3d 1376, 1383 (Fed. Cir. 2016) (conclusory statements are “insufficient articulations of motivation to combine” references). Dr. Nielsen’s expert statements do nothing to cure this deficiency, as Petitioners fail to “disclose [any] underlying facts or data on which the opinion is based[.]” *See* Pet. 81-83; EX1003, ¶249; *InfoBionic, Inc. v. Braemar Manufacturing, LLC*, IPR2015-01704, Paper 11, at 14-15 (P.T.A.B. Feb. 16, 2016) (denying institution) (citing 37 C.F.R. § 42.65(a)) (“Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.”). Thus, Petitioners and their expert fail to articulate any rationale rooted in fact or data as to why a POSITA would combine the mobile device authentication system of Aminzade with the dynamic biometric monitoring of Soli.

Therefore, a POSITA seeking to solve the problem addressed by the '228 Patent, preventing unauthorized use of a mobile device through coerced user access, would not have been motivated to combine Aminzade and Soli to arrive at the claimed invention. Soli is non-analogous art because the reference is in a separate field of endeavor and does not address the pertinent particular problem solved by Aminzade. **Soli teaches health monitoring and security measures directed to healthcare data privacy, while Aminzade teaches security measures directed to limiting user access of mobile device functionality.** Compare EX1004, Summary, 9:35-40, 23:28-34, 25:50-58, with EX1006, Abstract, ¶¶68, 225, 233-234, 469, and EX1007, ¶¶40, 140, 148-149, 165, 384. Combining these disparate teachings would not have logically led a POSITA to the claimed invention, particularly in the absence of any articulated rationale by Petitioners or their expert. As detailed below, such a combination still fails to disclose or suggest the key limitations of the challenged claims.

Therefore, a POSITA would not have been motivated to combine Aminzade with Soli.

2. The Combination of Aminzade and Soli Fails to Disclose Limitation [1.c] and [12.f]

In relation to these limitations, Petitioners merely cite back to limitations [1.c] and [12.f] in asserted Ground 1. Pet. 67, 78. Therefore, for the reasons provided

above in relation to limitations [1.c] and [12.f], Petitioners fail to establish that claim limitations [1.c] and [12.f] would have been rendered obvious in view of Aminzade and Soli. *See* § VII.A.2.

Therefore, Petitioners fail to establish a reasonable likelihood of success of any claim challenged in Ground 2.

3. The Combination of Aminzade and Soli Fails to Disclose Limitation [1.d] and [12.g]

In relation to these limitations, Petitioners cite back to limitation [1.c] in asserted Ground 1 to argue that Aminzade discloses “unlocking.” Pet. 68, 78. Therefore, for the reasons provided above in relation to limitations [1.c], [1.d] and [12.g], Petitioners fail to establish that claim limitations [1.d] and [12.g] would have been rendered obvious in view of Aminzade and Soli because Aminzade does not disclose an “unlocking” function. *See* §§ VII.A.2, VII.A.3.

Additionally, Petitioners argue that Soli's disclosure of the remaining limitation (*acquir[ing] the dynamic biometric information from the dynamic biometric information sensor*) would have been obvious to include “after” the “unlocking” mechanism. *See* Pet. 67-69. As set forth above, Aminzade does not disclose an “unlocking” operation. § VII.A.2. Even if it did, Petitioner's combination of Aminzade with Soli is impermissible hindsight. The '228 patent sets forth the necessity to include dynamic biometric information (“emotional biometrics”) in its

unlock operation to detect “a situation in which the user is threatened and forced to perform an illegal operation by a criminal[.]” EX1001 1:54-59. However, Soli does not take into account such a situation at all. See EX1006 ¶7 (mentioning user authorization only in the context of accessing wellness data on a device). For this and other reasons set forth above, Petitioner’s attempt to relate a lock/unlock operation to the acquisition of dynamic biometric information through combination of Aminzade with Soli is mere impermissible hindsight. See § VII.B.1. Thus, a POSITA would not be motivated to combine Aminzade and Soli to **acquire dynamic biometric information** after **unlocking**.

Therefore, Petitioners failed to establish a reasonable likelihood of success of any claim challenged in Ground 2.

4. The Combination of Aminzade and Soli Fails to Disclose Limitation [1.e] and [12.h]

In relation to these limitations, Petitioners cite back to limitation [1.e] in asserted Ground 1 to argue that Aminzade discloses “maintain[ing] an unlocked state during a condition.” Pet. 69-70, 78. Therefore, for the reasons provided above in relation to limitations [1.e] and [12.h], Petitioners fail to establish that claim limitations [1.e] and [12.h] would have been rendered obvious in view of Aminzade and Soli because Aminzade does not disclose “maintain[ing] an unlocked state” during any condition. See § VII.A.4.

Further, Petitioners rely solely on Aminzade to argue prior disclosure of “[a device] maintain[ing] an unlocked state during a condition,” and argue that Soli’s disclosure of the remaining limitation (*acquiring dynamic information*) would have been obvious to include as such a condition. *See* Pet. 69-70, 78. As set forth above, Aminzade does not disclose “maintain[ing] an unlocked state.” *See* § VII.A.4. Even if it did, Petitioner’s combination of Aminzade with Soli is impermissible hindsight. *See* §§ VII.B.1, VII.B.3. Thus, a POSITA would not be motivated to combine Aminzade and Soli to “maintain an unlocked state during a condition that dynamic biometric information can be acquired.”

Therefore, Petitioners failed to establish a reasonable likelihood of success of any claim challenged in Ground 2.

5. The Combination of Aminzade and Soli Fails to Disclose Claims 7 and 18

Claims 7 and 18 recite: “the first [information processing] device continuously acquir[ing] dynamic biometric information after being unlocked and the second [information processing] device receiv[ing] the dynamic biometric information transmitted from the first communication device continuously or based on starting of an application on the [second information processing] device.”

Because claim 7 depends from Claim 1, and claim 18 depends from claim 12, both claims include all the limitations that Aminzade in combination with Soli fail

to teach, as detailed *supra* § VII.B.2-4 (claim limitations [1.c], [1.d], [1.e], [12.f], [12.g], [12.h]). Petitioners' argument for claims 7 and 18 fails for at least these same reasons.

Specifically, Petitioners cite back to their arguments for claim limitation [1.d] to argue that Aminzade combined with Soli discloses "the first information processing device 'continuous[ly]' acquir[ing] the dynamic biometric information after being unlocked. *See* Pet. 76-77, 79. As set forth above, Aminzade does not disclose an "unlocking" operation, and a POSITA would not be motivated to combine Aminzade and Soli to continuously acquire dynamic biometric information after unlocking because Aminzade and Soli are not analogous art and solve different pertinent problems. *See* §§ VII.B.1, VII.B.2.

For at least the foregoing reasons, Petitioners fail to show a reasonable likelihood of success in establishing that claims 7 and 18 would have been rendered obvious in view of Aminzade in combination with Sowers.

C. Ground 3: Petitioners Fail To Establish That Claims 3, 10-11, 14, 21-22 are Rendered Obvious By Aminzade in View of Sowers and Hong

Claims 3, 10-11, 14, and 21-22 depend from Claims 1 and 12. Therefore, for at least the reasons provided above in relation to Claims 1 and 12 in Ground 1, Petitioners fail to establish that claims 3, 10-11, 14, and 21-22 would have been

rendered obvious based on Aminzade and Sowers. *See* § VII.A. Because Ground 3 is only asserted against dependent claims, Ground 3 inherently relies on Ground 1. *See* Pet. 84. Because Ground 1 fails, Ground 3 similarly fails for the reasons provided above in relation to Ground 1. *See* § VII.A.

1. No Motivation to Combine Aminzade with Hong

Additionally, Petitioners have not shown how a POSITA would have combined the teachings of Aminzade with the teachings of Hong with any expectation of success. Petitioners and their expert fail to articulate any rationale as to why a POSITA would combine the mobile device authentication system of Aminzade with the dynamic biometric monitoring of Hong. Petitioners simply provide conclusory statements that Hong's teaching of "an authentication method with an increased security level . . . when the wearer is sleeping" would have motivated a POSITA to add Hong's function to Aminzade's security authentication system merely because Aminzade discloses "increasing security" depending on whether a user is "wearing the wearable device[]." *See* Pet. 89-90; EX1008 ¶18; EX1009 ¶15; EX1004, 25:20-26:10. Petitioners' conclusory statements are insufficient and provide no factual support. *See* Pet. 89-90; *In re Nuvasive, Inc.*, 842 F.3d 1376, 1383 (Fed. Cir. 2016) (conclusory statements are "insufficient articulations of motivation to combine" references). Dr. Nielsen's expert statements

do nothing to cure this deficiency, as Petitioners fail to “disclose [any] underlying facts or data on which the opinion is based[.]” *See* Pet. 89-90; EX1003, ¶269; *InfoBionic, Inc. v. Braemar Manufacturing, LLC*, IPR2015-01704, Paper 11, at 14-15 (P.T.A.B. Feb. 16, 2016) (denying institution) (citing 37 C.F.R. § 42.65(a)) (“Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.”). Thus, Petitioners and their expert fail to articulate any rationale rooted in fact or data as to why a POSITA would combine the mobile device authentication system of Aminzade with the biometric authentication system of Hong.

D. Ground 4: Petitioners Fail To Establish That Claims 3, 10-11, 14, 21-22 are Rendered Obvious By Aminzade in View of Soli and Hong

Claims 3, 10-11, 14, and 21-22 depend from Claims 1 and 12. Therefore, for at least the reasons provided above in relation to Claims 1 and 12 in Ground 2, Petitioners fail to establish that claims 3, 10-11, 14, and 21-22 would have been rendered obvious based on Aminzade and Soli. *See* § VII.B.

Because Ground 4 is only asserted against dependent claims, Ground 4 inherently relies on Ground 2. *See* Pet. 90. Because Ground 2 fails, Ground 4 similarly fails for the reasons provided above in relation to Ground 2. *See* § VII.B.

Ground 4 also fails because, as explained above, Petitioners and their expert fail to articulate a motivation to combine Hong with Aminzade. *See* § VII.C.1.

E. Ground 5: Petitioners Fail To Establish That Claims 8-9, 19-20 are Rendered Obvious By Aminzade in View of Sowers and Altman

Claims 8-9 and 19-20 depend from Claims 1 and 12. Therefore, for at least the reasons provided above in relation to claims 1 and 12 in Ground 1, Petitioners fail to establish that claims 8-9 and 19-20 would have been rendered obvious based on Aminzade and Sowers. *See* § VII.A.

Because Ground 5 is only asserted against dependent claims, Ground 5 inherently relies on Ground 1. *See* Pet. 90. Because Ground 1 fails, Ground 5 similarly fails for the reasons provided above in relation to Ground 1. *See* § VII.A.

1. No Motivation to Combine Aminzade with Altman

Additionally, Petitioners have not shown how a POSITA would have combined the teachings of Aminzade with the teachings of Altman with any expectation of success. Altman is not analogous to Aminzade or the '228 Patent because they are in different fields of invention and do not seek to solve the same pertinent particular problem. Moreover, Petitioners and their expert fail to articulate any rationale as to why a POSITA would combine the mobile device authentication system of Aminzade with the location-aware social networking system of Altman.

Analogousness requires prior art to be in the “same field of endeavor” or “reasonably pertinent” to a similar problem being solved by the claimed invention. *In re Klein*, 647 F.3d 1343, 1348 (Fed. Cir. 2011) (citation omitted). The '228 Patent is directed to the field of “biometrics authentication,” to detect and prevent a situation where authentication may be carried out against a “user’s will” and a device may be “illegally operat[ed].” See EX1001, Summary of the Invention. In other words, the '228 Patent is directed towards enhancing security of a mobile device through an authentication system that limits access in situations where a user may be coerced to access the mobile device. See *id.*

A POSITA wouldn't be motivated to combine Aminzade with Altman because Altman is in a different field of endeavor than both the '228 Patent and Aminzade. Petitioners argue that Altman's disclosed location-based networking features, directed to “enhance the social networking capability of mobile devices and enhance the effectiveness of ad campaigns,” would have motivated a POSITA to combine Altman with Aminzade. Pet. 95-96; see also EX1010, 1:33-67. However, Altman exists in a different field of endeavor from both the '228 Patent and Aminzade. On one hand, Aminzade is directed to limiting or increasing user access to mobile device functionality based on user location and detection of the wearable device being worn to “increase security” of the mobile device. EX1004, Summary,

9:35-40, 23:28-34, 25:50-58. On the other hand, Altman discloses an invention related to “mobile communication networks, and more specifically, to displaying location-based advertising links and messages on a mobile device.” EX1010, Field, 1:26-29. Unlike Aminzade, Altman does not disclose altering security access to a mobile device's applications or functionality. *See generally id.* Rather, Altman exists in a wholly different field of endeavor because Altman is directed to location-based social networking between mobile devices. *See id.* at Abstract, Field, 1:26-29. Thus, Petitioners' proposed combination of Altman and Aminzade fails the first test for analogousness because Altman exists in a separate field of endeavor from both Aminzade and the '228 Patent.

Further, a POSITA wouldn't be motivated to combine Aminzade with Altman because Altman solves different pertinent problems than both Aminzade and the '228 Patent, failing the second test for analogousness. *See In re Klein*, 647 F.3d 1343, 1348 (Fed. Cir. 2011) (“A reference is reasonably pertinent if, even though it may be in a different field [of endeavor]. . . it is one which . . . logically would have commended itself to an inventor's attention in considering his problem.”) (citation omitted). The '228 Patent's disclosed purpose is to detect and prevent a situation where authentication may be carried out against a “user's will” or “intension.” *See* EX1001, Summary of the Invention. Additionally, Aminzade discloses limiting or

increasing user access to mobile device functionality based on user location and detection of the wearable device being worn, for the disclosed purpose of “increas[ing] security” to the mobile device functionality. EX1004, Summary, 9:35-40, 23:28-34, 25:50-58. In contrast, Altman is directed to “enhance the social networking capability of mobile devices and enhance the effectiveness of ad campaigns.” See Pet. 95-96; see EX1010, 1:33-67. Petitioners argue that Altman’s disclosed location-based features would have motivated a POSITA to combine Altman with Aminzade. Pet. 95-96; see also EX1010, 1:33-67. However, Aminzade does not mention anything about social networking capabilities between devices, nor does it make any mention of enhancing the effectiveness of ad campaigns. See EX1010, 1:33-67. See generally EX1004. Aminzade discloses **limiting access to a mobile device’s applications and functionality for enhancing user security**, and is distinct from Altman’s teaching directed to **enhancing the social networking capability of mobile devices and the effectiveness of ad campaigns**. Compare EX1004, Summary, 9:35-40, 23:28-34, 25:50-58 (disclosing purpose of “increas[ing] security” to mobile device functionality) with EX1010, 1:33-67 (teaching enhancement of social networking capability of mobile devices and effectiveness of ad campaigns). Thus, Aminzade is directed towards solving a different pertinent problem than Altman, failing the second test of analogousness.

Moreover, Petitioners and their expert fail to articulate any rationale as to why a POSITA would combine the mobile device authentication system of Aminzade with the location-aware social networking system of Altman. Petitioners simply provide conclusory statements that Altman's disclosed location-based features, directed to "enhance the social networking capability of mobile devices and enhance the effectiveness of ad campaigns," would have motivated a POSITA to combine Altman with Aminzade. Pet. 95-96; *see also* EX1010, 1:33-67. Petitioners' conclusory statements are insufficient and provide no factual support. *See* Pet. 95-96; *In re Nuvasive, Inc.*, 842 F.3d 1376, 1383 (Fed. Cir. 2016) (conclusory statements are "insufficient articulations of motivation to combine" references). Dr. Nielsen's expert statements do nothing to cure this deficiency, as Petitioners fail to "disclose [any] underlying facts or data on which the opinion is based[.]" *See* Pet. 95; EX1003, ¶284; *InfoBionic, Inc. v. Braemar Manufacturing, LLC*, IPR2015-01704, Paper 11, at 14-15 (P.T.A.B. Feb. 16, 2016) (denying institution) (citing 37 C.F.R. § 42.65(a)) ("Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight."). Thus, Petitioners and their expert fail to articulate any rationale rooted in fact or data as to why a POSITA would combine the mobile device authentication system of Aminzade with the location-aware social networking system of Altman.

Therefore, a POSITA seeking to solve the problem addressed by the '228 Patent, preventing unauthorized use of a mobile device through coerced user access, would not have been motivated to combine Aminzade and Altman to arrive at the claimed invention. Altman is non-analogous art because the reference is in a separate field of endeavor and does not address the pertinent particular problem solved by the '228 Patent or Aminzade. **Altman teaches enhancing the social networking capability of mobile devices, while Aminzade teaches enhancing security measures directed to user access of mobile device functionality.** Compare EX1004, Summary, 9:35-40, 23:28-34, 25:50-58, with EX1010, 1:33-67. Combining these disparate teachings would not have logically led a POSITA to the claimed invention, particularly in the absence of any articulated rationale by Petitioners or their expert.

Therefore, a POSITA would not have been motivated to combine Aminzade with Altman.

F. Ground 6: Petitioners Fail To Establish That Claims 8-9, 19-20 are Rendered Obvious By Aminzade in View of Soli and Altman

Claims 8-9 and 19-20 depend from Claims 1 and 12. Therefore, for at least the reasons provided above in relation to claims 1 and 12 in Ground 2, Petitioners fail to establish that claims 8-9 and 19-20 would have been rendered obvious based on Aminzade and Soli. See § VII.B.

Because Ground 6 is only asserted against dependent claims, Ground 6 inherently relies on Ground 2. *See* Pet. 96. Because Ground 2 fails, Ground 4 similarly fails for the reasons provided above in relation to Ground 2. *See* § VII.B. Ground 6 also fails because, as explained above, Petitioners and their expert fail to articulate a motivation to combine Hong with Aminzade. *See* § VII.E.1.

VIII. CONCLUSION

For at least the foregoing reasons, the Board should deny institution of the Petition.

Dated: December 5, 2025

Respectfully submitted,

/Robert G. Pluta /
Robert G. Pluta (Reg. No. 50,970)
MAYER BROWN LLP
71 S. Wacker Drive
Chicago, IL 60606
Telephone: (312) 701-8641
Fax: (312) 706-8144

Saqib J. Siddiqui (Reg. No. 68,626)
MAYER BROWN LLP
1999 K Street NW
Washington DC, 20006
ssiddiqui@mayerbrown.com

Counsel for Maxell, Ltd.

Case IPR2025-01313
Patent No. 10,783,228
Patent Owner's Preliminary Response

CERTIFICATE OF SERVICE

I hereby certify that on this 5th day of December, 2025, a copy of the attached
PATENT OWNER PRELIMINARY RESPONSE TO PETITION FOR *INTER*
PARTES REVIEW OF U.S. PATENT NO. 10,783,228, together with all exhibits
was served by electronic mail to the attorneys of record, at the following addresses:.

Robert Buergi
robert.buergi@dlapiper.com

Chris Katsantonis
chris.katsantonis@dlapiper.com

With a courtesy copy by electronic mail to:
DLA-Maxell-2-IPRs@us.dlapiper.com

Respectfully submitted,

Date: December 5, 2024

By: /Robert G. Pluta/
Robert G. Pluta (Reg. No. 50,970)

Counsel for Maxell, Ltd.

CERTIFICATION PURSUANT TO 37 C.F.R. § 42.24(d)

Pursuant 37 CFR 42.24(d), the undersigned certifies that this Preliminary Response and complies with the type-volume limitation of 37 CFR §42.24(a). The word count application of the word processing program used to prepare this Preliminary Response indicates that the Preliminary Response contains 12,630 words, excluding the parts of the brief exempted by 37 C.F.R. § 42.24(a).

Respectfully submitted,

/Robert G. Pluta/

Robert G. Pluta (Reg. No. 50,970)
Mayer Brown, LLP
71 S. Wacker Drive
Chicago, IL 60606
Telephone: (312) 701-8641
Fax: (312) 706-8144
rpluta@mayerbrown.com