

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

EXPERIAN INFORMATION SOLUTIONS, INC.,

Petitioner,

v.

DYNAPASS IP HOLDINGS, LLC

Patent Owner.

***Inter Partes* Review No. IPR2023-01406**

Patent No. 6,993,658

**PATENT OWNER'S PRELIMINARY RESPONSE TO THE PETITION
FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 6,993,658
PURSUANT TO 37 C.F.R. § 42.107**

Filed on behalf of Patent Owner by:

John Wittenzellner (Reg. No. 61,662)
1735 Market Street, Suite A #453
Philadelphia, PA 19103

Mark McCarthy (Reg. No. 69,575)
601 Congress Ave., Suite 600
Austin, TX 78701

WILLIAMS SIMONS & LANDIS PLLC

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	STATEMENT OF THE PRECISE RELIEF REQUESTED	3
III.	THE PETITION SHOULD BE DENIED BECAUSE IT DOES NOT ESTABLISH A REASONABLE LIKELIHOOD OF SUCCESS ON ANY CHALLENGED CLAIM.	3
A.	The '658 Patent.....	4
B.	Level of Ordinary Skill in the Art	11
C.	Claim Construction.....	11
D.	Ground 1 – The Combination of <i>Sormunen</i> and <i>Perlman</i> Does Not Render Obvious Claims 1-7 of the '658 Patent.....	12
1.	Independent Claim 1	17
i.	[1.c] “receiving a request . . . for a token . . . over the second network”	17
ii.	[1.d] “generating a new password . . . based at least upon the token and a passcode . . .”	20
iii.	[1.f] “activating access the user account on the first secure computer network”	27
iv.	[1.h] “receiving the password from the user via the first secure computer network”	30
v.	[1.i] “deactivating access to the user account . . . within a predetermined amount of time after said activating . . .”	31
2.	Dependent Claims 2-4.....	34
3.	Independent Claim 5	35

i.	[5.d] “a control module . . . configured to create a new password based at least upon a token and a passcode . . .”	35
ii.	[5.f] “an authentication module configured to receive the password from the user . . . wherein the authentication module activates access to the account in response to the password and deactivates the account within a predetermined amount of time after activating the account . . .”	36
4.	Dependent Claims 6 and 7	40
IV.	THE BOARD SHOULD EXERCISE ITS DISCRETION TO DENY THE PETITION.	40
A.	The Board Should Exercise Its Discretion to Deny the Petition Under 35 U.S.C. § 314(a).	43
1.	General Plastic Factor One	44
2.	General Plastic Factor Two.....	47
3.	General Plastic Factor Three.....	48
4.	<i>General Plastic</i> Factors Four and Five	49
5.	<i>General Plastic</i> Factor Six and Seven	50
B.	The Board Should Exercise Its Discretion to Deny the Petition Under 35 U.S.C. § 325(d).	51
1.	The First Part of the Framework is Satisfied by Every Reference Asserted in the Petition.....	52
2.	The Second Part of the Framework is Satisfied, So Institution Should be Denied.	52
V.	THE PETITION SHOULD BE DENIED BECAUSE THE BOARD DOES NOT HAVE JURISDICTION OVER EXPIRED PATENTS.....	53
VI.	CONCLUSION.....	55

TABLE OF AUTHORITIES

Cases

<i>Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH,</i> IPR2019-01469, Paper 6 (P.T.A.B. Feb. 13, 2020) (precedential)	52
<i>Apple Inc. v. Uniloc 2017 LLC,</i> IPR2020-00854, Paper 9 (P.T.A.B. Oct. 28, 2020) (precedential)	48
<i>Cuozzo Speed Techs., LLC v. Lee,</i> 136 S. Ct. 2131 (2016)	43
<i>Ericsson Inc. v. Uniloc 2017, LLC,</i> IPR2019-01550, Paper 8 (Mar. 17, 2020)	45, 46
<i>General Plastic Indus. Co. v. Canon Kabushiki Kaisha,</i> IPR2016-01357, Paper 19 (P.T.A.B. Sept. 6, 2017) (precedential)	passim
<i>In re Ratti,</i> 270 F.2d 810 (CCPA 1959)	26
<i>Meiresonne v. Google, Inc.,</i> 849 F.3d 1379 (Fed. Cir. 2017)	25
<i>NetApp Inc. v. Realtime Data LLC,</i> IPR2017- 01195, Paper 9 (P.T.A.B. Oct. 12, 2017)	45
<i>Oil States Energy Servs., LLC v. Greene’s Energy Grp., LLC,</i> 138 S. Ct. 1365 (2018)	53
<i>Valve Corp. v. Electronic Scripting Products, Inc.,</i> IPR2019-00064, Paper 10 (P.T.A.B. May 1, 2019) (precedential)	50
<i>Valve Corporation v. Electronic Scripting Products, Inc.,</i> IPR2019-00062, Paper 11 (P.T.A.B. April 2, 2019) (precedential)	45, 51

Statutes

35 U.S.C. § 314	43, 55
35 U.S.C. § 325	51, 53, 55

Other Authorities

MPEP § 2143	26
-------------------	----

Rules

37 C.F.R. § 42.100	39
--------------------------	----

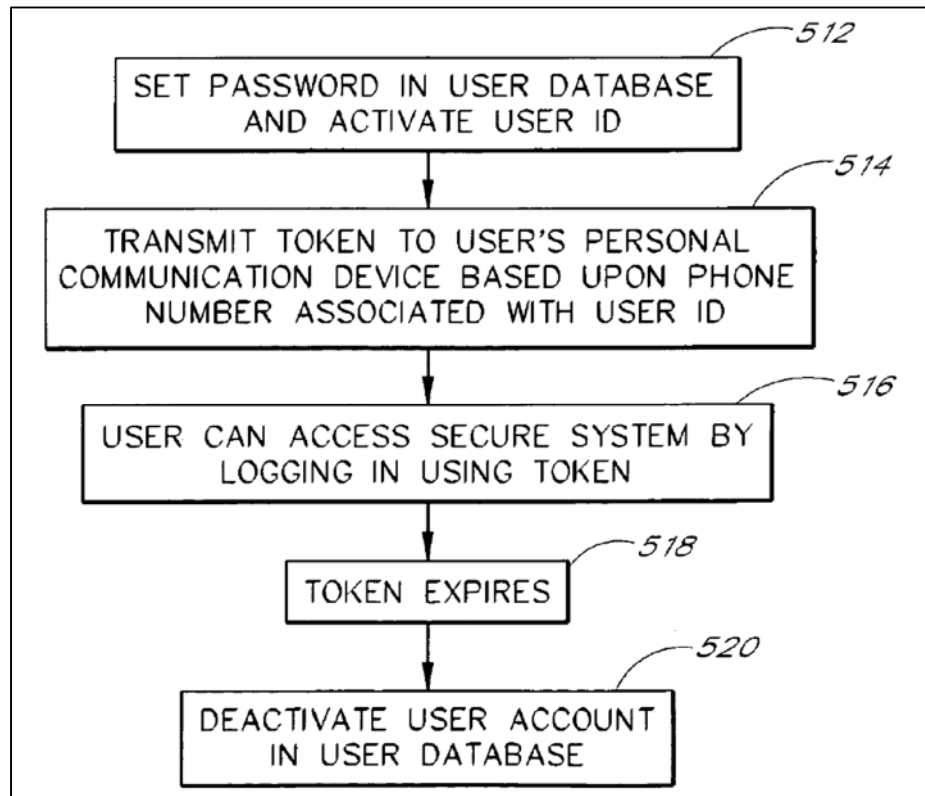
EXHIBIT LIST

Exhibit	Description
2001	Google Patents webpage for U.S. Patent No. 6,993,658, https://patents.google.com/patent/US6993658B1/
2002	Claim Construction Order, <i>Dynapass Holdings LLC v. JPMorgan Chase & Co., et al.</i> , Case No. 2:22-cv-00212-JRG-RSP, Dkt. 120 (E.D. Tex. Oct. 31, 2023).
2003	Proof of Service of Summons in Civil Action, <i>Dynapass IP Holdings LLC v. Experian Information Services, Inc.</i> , Case No. 2:23-cv-00066 (E.D. Tex.).

I. INTRODUCTION

Dynapass IP Holdings, LLC (“Patent Owner”) respectfully submits this Preliminary Response (the “Response”) to the Petition for *Inter Partes* Review of U.S. Patent No. 6,993,658 (Paper 1, the “Petition” or “Pet.”) filed by Experian Information Solutions, Inc. (“Petitioner”). The ’658 Patent relates to “the authentication of users of secure systems and, more particularly, the invention relates to a system through which user tokens required for user authentication are supplied through personal communication devices such as mobile telephones and pagers.” Ex. 1001 at 1:7-11.

Institution should be denied because the Petition fails to demonstrate a reasonable likelihood that any challenged claim of the ’658 Patent is unpatentable. As detailed herein, the combination of references applied by the Petition against the independent claims of the ’658 Patent has numerous glaring deficiencies. For example, the independent claims require activation of the user’s account in response to creation of a new “password” for the user (the “password” in the claims is “based at least upon a token and a passcode”). The account remains active until the expiration of “a predetermined amount of time after activating the account.” That process is depicted in Figure 5, a portion of which is reproduced below:



Ex. 1001, Fig. 5 (excerpted).

The asserted references do not discuss activation of a user account. Putting that aside, Petitioner disregards the requirement that activation occurs in response to creation of a new “password” for the user.

In addition, the Petition constitutes nothing more than the third bite of the apple in an attempt to invalidate the claims of the '658 Patent. Petitioner delayed its filing until seven months after being served with a complaint, only to retread over familiar ground by asserting prior art that has been considered by the Patent Office during prosecution and *inter partes* review proceedings. As a result, the Petition satisfies both the (1) *General Plastic* factors and (2) the two-part framework of 35

U.S.C. § 325(d). Accordingly, the Board should exercise its discretion to deny institution.

Finally, institution should be denied because the Board does not have jurisdiction over expired patents. For these reasons, institution should be denied.

II. STATEMENT OF THE PRECISE RELIEF REQUESTED

Petitioner asserts that claims 1-7 of the '658 Patent are unpatentable under the following grounds:

Ground	References	Challenged Claims
1	<i>Sormunen</i> in view of <i>Perlman</i>	1-7

Pet., p. 15.

Patent Owner requests that the Board deny institution of the Petition with respect to all challenged claims and all asserted grounds. A full statement of the reasons for the relief requested is set forth in Sections III, IV, and V of this Response.

III. THE PETITION SHOULD BE DENIED BECAUSE IT DOES NOT ESTABLISH A REASONABLE LIKELIHOOD OF SUCCESS ON ANY CHALLENGED CLAIM.

As shown below, the Petition fails to demonstrate a reasonable likelihood that Petitioner would prevail with respect to any claim of the '658 Patent. The Petition challenges claims 1-7 of the '658 Patent (the "Challenged Claims"). Pet. at 15. As

detailed herein, the proposed Ground fails to disclose key limitations of each Challenged Claim, so trial should not be instituted.

A. The '658 Patent

The '658 Patent, which is titled “Use of Personal Communication Devices for User Authentication,” was filed on March 6, 2000, and issued on January 31, 2006. Ex. 1001. The '658 Patent relates to “the authentication of users of secure systems and, more particularly, the invention relates to a system through which user tokens required for user authentication are supplied through personal communication devices such as mobile telephones and pagers.” Ex. 1001 at 1:7-11.

At the time of the claimed inventions, “secure systems”¹ used “a user ID and password pair to identify and authenticate system users.” *See id.* at 1:13-14. Although user ID/password pairs were ubiquitous, they suffered from several shortcomings, as recognized by the inventors of the '658 Patent:

Passwords created by users are often combinations of words and names, which are easy to remember but also easily guessed. Guessing passwords is a frequent technique used by “hackers” to break into systems. Therefore, many systems impose regulations on password formats that require mixtures of letters of different cases and symbols and that no part of a password be a word in the dictionary. A user’s inability to remember complex combinations of letters, numbers, and

¹The '658 Patent describes many non-limiting examples of a “secure system,” including Novell NetWare-, Microsoft NT-, Windows 2000-, and UNIX/Linux-based computers, as well as “any system, device, account, . . . a user account on a network of computer workstations, a user account on a website, or a secure area of a building.” Ex. 1001 at 1:13-19, 4:13-23.

symbols often results in the password being written down, sometimes on a note stuck to the side of a workstation.

Id. at 1:28-38.

The increasing use of remote connectivity at the time of the claimed inventions further exacerbated the shortcomings of user ID/password pairs. *See id.*

at 1:20-26. As a result, then-current systems faced several issues:

Present systems face several problems: users dread frequent password changes, frequent password changes with hard-to-remember passwords inevitably result in users surreptitiously writing down passwords, and security is compromised when users write down their passwords.

Id. at 1:39-43. Two-factor authentication (a form of multi-factor authentication) improves user ID/password pairs by adding “unpredictable, one-time-only access codes.” *See id.* at 1:49-51. The first factor is “a user passcode or personal identification number.” *See id.* at 1:46-47. The second factor is the “unpredictable, one-time-only access codes.” *See id.* at 1:49-51. In two-factor authentication, system access is based upon:

- “nonsecret information known to the user, such as the user ID;”
- secret information known to the user, such as the passcode;” and
- “information provided to the user through an object possessed by the user, such as the token.”

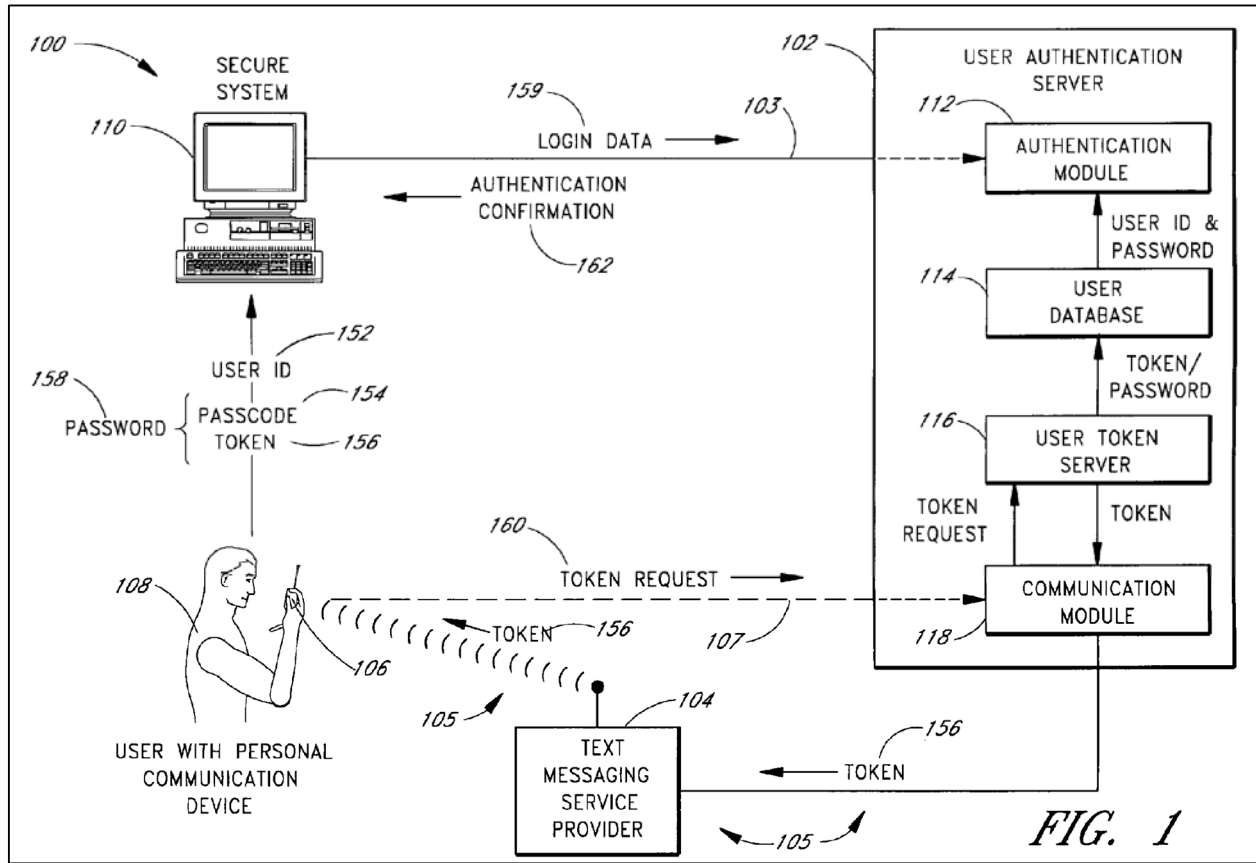
Id. at 2:11-15.

The '658 Patent acknowledges the existence of the RSA Security, Inc. SecurID product at the time of the claimed inventions, but identified significant deficiencies in the product:

The SecurID product, however, requires users to carry an additional item on their person in order to access a secure system. It would be advantageous if the benefits of the SecurID system could be achieved using a device that many users already carry—a personal communication device such as a mobile phone or a pager.

Id. at 1:54-59. The '658 Patent requires the use of a personal communication device, which teaches away from a separate device like the SecurID product. *See id.*

The '658 Patent solves the deficiencies of the SecurID product and further improves two-factor authentication in a unique, novel, non-obvious way. Figure 1 of the '658 Patent, reproduced below, depicts an embodiment of a user authentication system (identified as “100” in the figure):



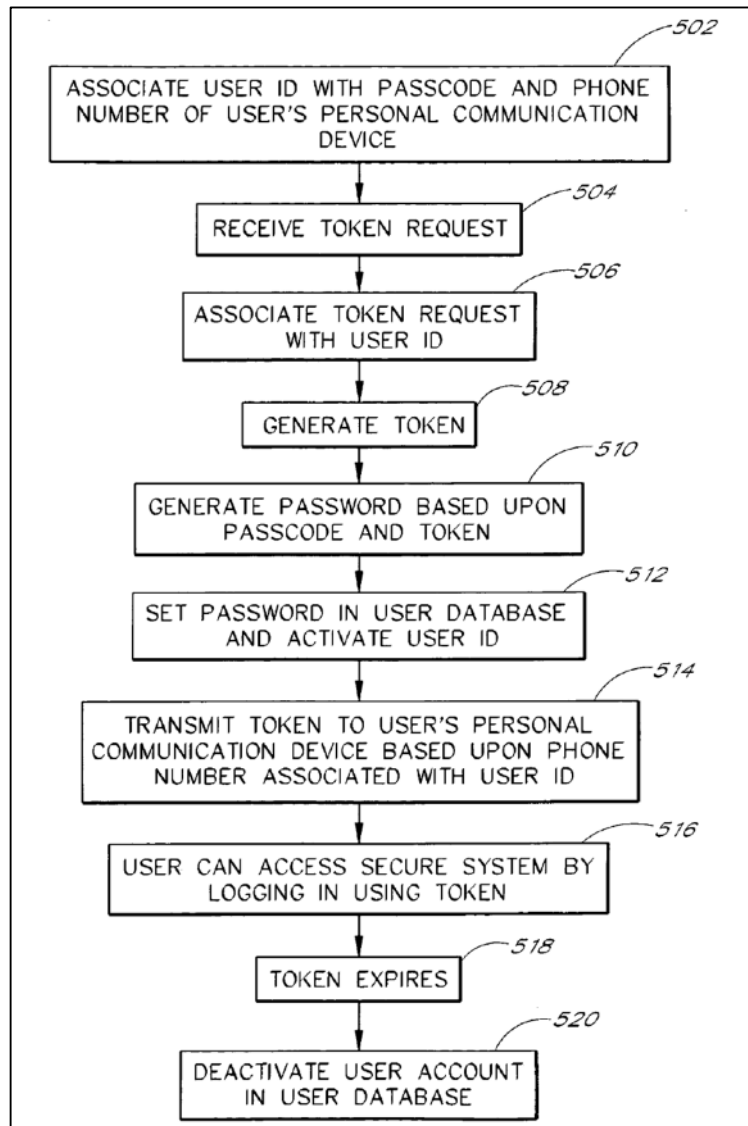
Id. at Fig. 1; *see also id.* at 3:31-33.

Authentication system (100) regulates access to secure system (110). *Id.* at 4:9-13. User authentication server (102) “preferably includes a program or a suite of programs running on a computer system to perform user authentication services.” *Id.* at 4:27-29. “The authentication information preferably includes a user ID 152, a passcode 154 and a user token 156.” *Id.* at 4:36-39. Tokens are received on the user’s personal communication device (106), which can be, for example, “a pager or mobile phone having SMS (short message service) receive capability.” *Id.* at 4:13-15.

It is important to be aware of the terminology used by the '658 Patent. The “user ID may be publicly known and used to identify the user.” *Id.* at 4:39-40. The '658 Patent uses the term “passcode” to refer to what is commonly called a “password:” “For example, the user 108 can combine a valid, memorized passcode of ‘abcd’” *Id.* 4:54-55; *see also id.* at 1:27-29 (“Passwords created by users are often combinations of words and names, which are easy to remember but also easily guessed.”), 4:40 (The passcode 154 is preferably secret and known only to the user 108.”). The “token” can be, for example, “a random or pseudo-random sequence of numbers or digits or both numbers and digits.” *Id.* at 9:22-24.

The '658 Patent uses the term “password” to refer to the combination of at least the “passcode” and a “token.” *Id.* at 4:52-53 (“In the preferred embodiment, the user 108 combines the token 156 with the passcode 154 to form a password 158.”). For example, if the passcode is “abcd” and the token is “1234,” the password could be “abcd1234” or “1234abcd.” *See id.* at 4:54-56. The components of the password (e.g., the passcode and token) can be combined or sent to the system as separate components. *See id.* at 4:52-65.

Figure 5, reproduced below, depicts an embodiment of how the system provides tokens and authenticates users.



Id. at Fig. 5; *see also id.* at 3:41-43.

In step 502, the system associates the user's user ID and passcode with the user's personal communication device. *Id.* at 8:53-60. By doing so, the system transmits the token only to the associated user. *See id.* In steps 504, 506, and 508, the system receives a request for a token, determines which user made the request (i.e., associates the request with a user ID), and generates the token. *See id.* at 9:3-

27, Fig. 5. Those steps differ from other systems that continually generate access codes. *See, e.g., id.* at 1:49-51 (“The SecurID card generates and displays unpredictable, one-time-only access codes that automatically change every 60 seconds.”). In step 510, the system generates a new “password” based on at least the “token” and “passcode.” *Id.* at 9:28-33, Fig. 5. That password is then stored and the user’s account can be activated if it was deactivated. *Id.* at 9:34-41, Fig. 5 (step 512).

In step 514, the system transmits the token to the user’s personal communication device. *See id.* at 9:44-53, Fig. 5. Claim 1 of the ’658 Patent requires that the “personal communication device” be “in communication over a second network, wherein said network is a cell phone network. . . .” *Id.* at 11:47-50. Claim 5 requires that the token is transmitted to the “personal communication device” through a “cell phone network.” *Id.* at 12:34-36. The claims also require that the user’s account is deactivated “within a predetermined amount of time” after the account is activated. *Id.* at 12:9-13 (claim 1), 12:41-47 (claim 5).

The Patent Office issued the ’658 Patent issued after several office actions. Since then, the ’658 Patent has been cited by more than 200 patent applications. Ex. 2001, <https://patents.google.com/patent/US6993658B1/>. Amongst those patent applications are patent applications filed by major industry entities, including IBM Corporation, Microsoft Corporation, Lucent Technologies, Honeywell International,

Inc., British Telecommunications PLC, AT&T, Visa, and Google Inc. *See id.* They also include a patent application filed by JPMorgan Chase Bank, N.A., a defendant in the parallel district court proceedings in the Eastern District of Texas. *See id.*

B. Level of Ordinary Skill in the Art

For the purposes of this Response only, Patent Owner does not dispute the level of skill of a person of ordinary skill in the art (“POSITA”) identified in the Petition. *See* Pet., p. 14. Patent Owner notes, however, that the United States District Court for the Eastern District of Texas found that a POSITA would have at least an undergraduate degree in electrical engineering, computer science, computer engineering, or a closely related field, and two years experience in online security, such as user authentication technologies. Ex. 2002 at 6-7.

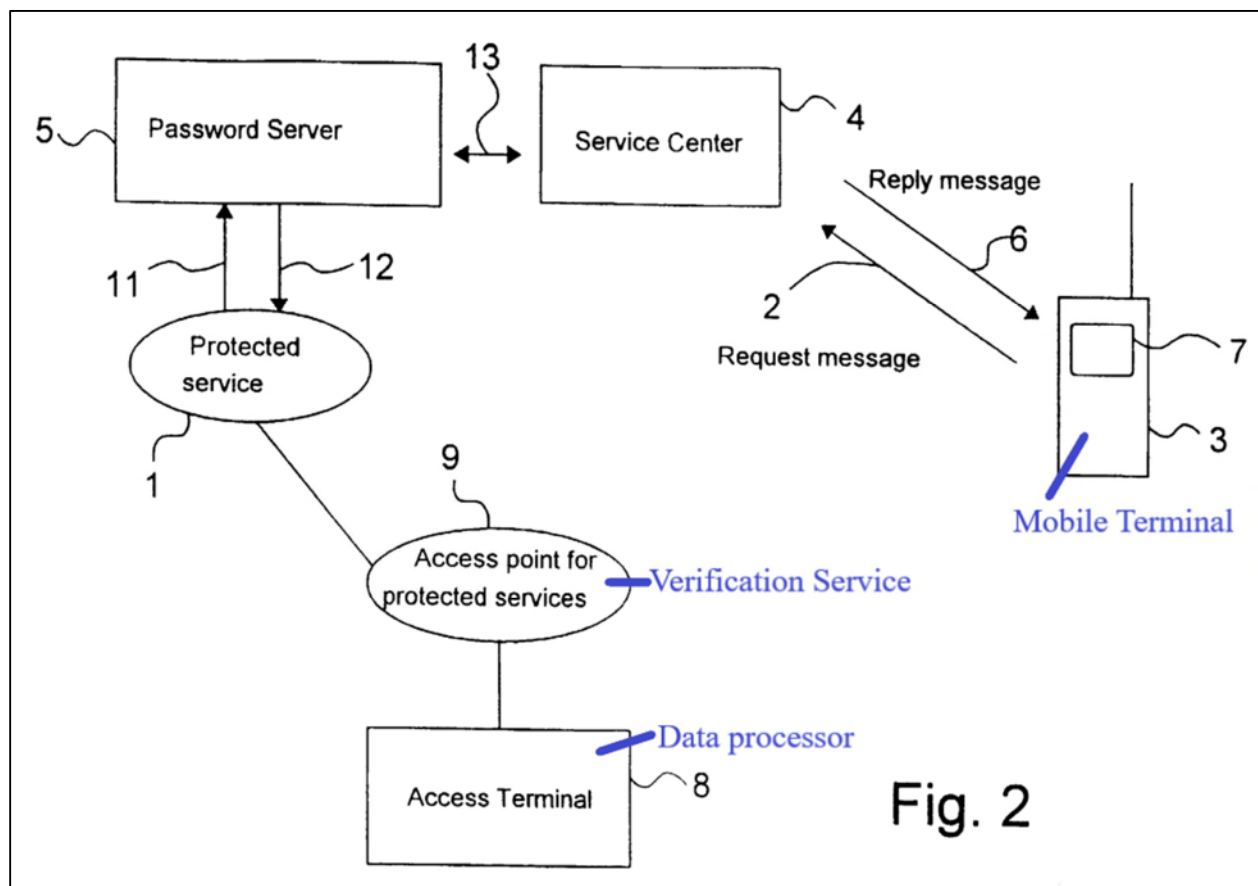
C. Claim Construction

Except as noted below, Patent Owner contends that claim construction is not necessary for the Board to determine that the Petition fails to demonstrate a reasonable likelihood that any challenged claim of the ’658 Patent is unpatentable. Patent Owner reserves the right to address claim construction of any term in the challenged claims if the Board institutes *inter partes* proceedings.

D. Ground 1 – The Combination of *Sormunen* and *Perlman* Does Not Render Obvious Claims 1-7 of the '658 Patent.

Petitioner contends that the combination of *Sormunen* and *Perlman* renders obvious claim 1-7 of the '658 Patent. Pet. at 15, 28-47. That combination does not render obvious claims 1-7 of the '658 Patent for at least the following reasons.

Sormunen discloses a system for obtaining passwords for a “protected service 1.” See Ex. 1004, 1:1-5, Fig. 2. The system includes a user’s “access terminal 8,” a user’s “mobile terminal 3,” a “service center 4,” and a “password server 5.” See Ex. 1004, 5:35-7:18, Fig. 2. Figure 2 of *Sormunen* is reproduced below:



Ex. 1004, Fig. 2 (annotated). To use “protected service 1,” the user “sends a short message 2” including “a password request and possibly also a subscription request for a new user” from the “mobile terminal 3” to “service center 4.” *See* Ex. 1004, 5:35-6:3, Fig. 2. The “service center 4 processes the incoming messages . . . and transmits the inquiry” to “password server 5.” *See* Ex. 1004, 6:20-23, Fig. 2. The “password server 5 transmits the password and/or the user name to the [] service center 4, which forms . . . a reply message 6, which is sent to the [mobile] terminal 3.” Ex. 1004, 6:35-37, Fig. 2. The password in “reply message 6” may be displayed to the user on the “mobile terminal.” Ex. 1004, 7:4-6, Fig. 2.

The user forms a connection between “data processor 8” and “a verification service 9 of the [protected] service 1.” *See* Ex. 1004, 7:9-10, Fig. 2. The user name and password (as set forth in “reply message 6”) are transmitted by “data processor 8” to the “password server 5” via the “verification service 9.” *See* Ex. 1004, 7:11-14, Fig. 2. The “password server 5” determines “whether the user name and the password are given correctly.” Ex. 1004, 7:14-16, Fig. 2. If the user name and password are correct, the user is given access to “protected service 1.” Ex. 1004, 7:16-18, Fig. 2.

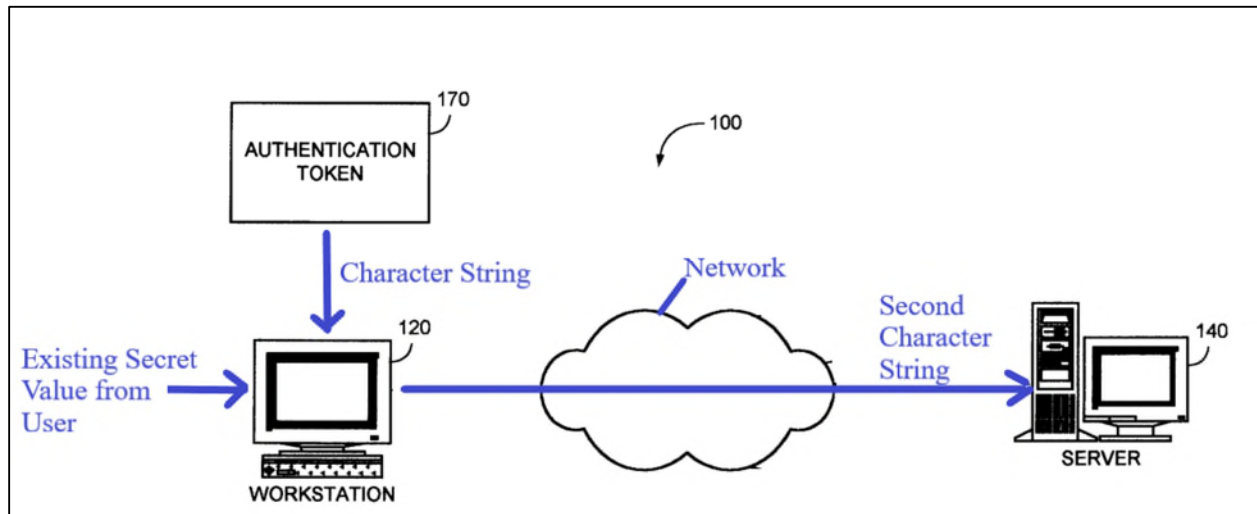
Through that mechanism *Sormunen*’s system purportedly provides “fast and safe[]” transmission of at least a password to the user. Ex. 1004, 4:18-21. “A

further advantage of the fast data transmission is that the validity of passwords can be shortened remarkably and security may thus be improved.” Ex. 1004, 5:16-18.

Sormunen also discloses one embodiment for “obtaining a personal identity number (PIN) of bank and credit cards and corresponding charge cards. Thus when the charge card is being ordered, the number of the orderer’s paging device or mobile station can be given, wherein the supplier of the charge card transmits the personal identity number connected to the charge card to the paging device or the mobile station of the user.” Ex. 1004, 9:26-32.

But *Sormunen* fails to disclose at least generating a “new password” based on a “token” and a “passcode,” as independent claims 1 and 5 require. Further, *Sormunen* fails to disclose deactivating access to a user account “within a predetermined amount of time after activating the account,” as independent claims 1 and 5 also require. Further still, *Sormunen* fails to disclose “receiving a request . . . for a token via the personal communication device,” over a cell phone network, as independent claim 1 requires.

Perlman discloses a “system 100” including an “authentication token 170,” a “workstation 120” and a “server 140.” Ex. 1005, 4:65-5:8, Fig. 1. Figure 1 of *Perlman* is reproduced below:



Ex. 1005, Fig. 1 (excerpted and annotated). *Perlman* discloses generating a “character string” using time-synchronized “authentication token 170.” *See* Ex. 1005, 4:38-55, 8:55-9:9, Fig. 1. The “character string” is communicated to “workstation 120” along with an existing secret value known to the user. *See* Ex. 1005, 4:38-55, 8:55-9:9, Fig. 1. The “workstation 120” generates a “second character string” based on the existing secret value known to the user and the “character string” from the time-synchronized “authentication token 170.” *See id.* The “workstation 120” transmits the “second character string” from the “workstation 120” to “server 140” to authenticate the user. *See id.* *Perlman*’s system has an enhanced or “more secure” password because a new “character string” from the time-synchronized “authentication token 170” is used each time the user needs to be authenticated. *See* Ex. 1005, 6:20-38 (“the character string is the time of day in minutes . . . To allow for clock skew and delays in typing and transmission, the

server will accept any one of several character strings, based on character strings the token might have displayed in the last seven minutes or the next three minutes”). In other words, *Perlman*’s “character string” is only good for a single authentication attempt.

But *Perlman* fails to disclose at least deactivating access to a user account “within a predetermined amount of time after activating the account,” as independent claims 1 and 5 require. Further, *Perlman* fails to disclose “transmitting the token to the personal communication device” through the cell phone network as independent claims 1 and 5 also require. Further still, *Perlman* fails to disclose “receiving a request . . . for a token via the personal communication device,” over a cell phone network, as independent claim 1 requires.

Additionally, *Perlman*’s “authentication token” is similar to RSA’s SecurID product disclosed in the ’658 Patent. See Ex. 1001, 1:44-59. Both *Perlman*’s “authentication token” and RSA’s SecurID product are additional devices (i.e., not the user’s cellphone, not the user’s pager) that the user must carry with him/her and that locally generate one-time access codes based on time, not receiving the token. Compare Ex. 1005, 5:46-64, 6:20-38 with Ex. 1001, 1:44-59. But the ’658 Patent expressly discloses the claimed invention is designed to operate with the user’s personal communication device to save the user from having to carry around yet another device like RSA’s SecurID product, and thus *Perlman*’s “authentication

token.” *See* Ex. 1001, 1:56-59 (“It would be advantageous if the benefits of the SecurID system could be achieved using a device that many users already carry—a personal communication device such as a mobile phone or a pager.”) (emphasis added). Accordingly, *Perlman* with its necessary “authentication token” teaches away from the claimed invention. Moreover, by relying on *Perlman*, the Petition is effectively taking the same prior art (i.e., RSA’s SecurID product) and recasting it through impermissible hindsight.

1. Independent Claim 1

The combination of *Sormunen* and *Perlman* does not render obvious independent claim 1 because the combination does not teach or suggest the following elements of the claim.

- i. [1.c] “receiving a request . . . for a token . . . over the second network”

Claim element [1.c] recites “receiving a request from the user for a token via the personal communication device, over the second network.” The “second network” is a “cell phone network.” *Compare* claim element [1.c] *with* claim element [1.b] (“wherein said second network is a cell phone network”). Petitioner mapped *Sormunen*’s “short [request] message 2” from the “mobile terminal” to the claimed “request from the user” and “personal communication device,” respectively. *See* Pet. at 32-33. Petitioner also mapped *Sormunen*’s “PIN” of a bank/credit card to the claimed “token.” *See* Pet. at 34 (“the new password to be combination of the

known password (passcode) and the PIN (token))” (emphasis added). But *Sormunen* fails to disclose that the “short [request] message 2” (the identified “request from the user”) is a request for the “PIN” (the identified “token”), as claim element [1.c] requires.

Sormunen discloses that “[t]he short [request] message 2 includes a password request and possibly also a subscription request for a new user.” Ex. 1004, 5:38-6:2. But neither a “password request” nor a “subscription request” is the same as a request for *Sormunen*’s “PIN” (the identified “token”). In fact, Petitioner concedes that *Sormunen*’s “password” and *Sormunen*’s “PIN” are not the same. See Pet. at 34 (“A POSA would have found it obvious for the new password to be combination of [*Sormunen*’s] known password (passcode) and [*Sormunen*’s] PIN (token)”). Accordingly, *Sormunen* fails to disclose claim element [1.c].

Further, *Sormunen* also discloses

the present invention can be applied also for obtaining a personal identity number (PIN) of bank and credit cards and corresponding charge cards. Thus when the charge card is being ordered, the number of the orderer’s paging device or mobile station can be given, wherein the supplier of the charge card transmits the personal identity number connected to the charge card to the paging device or the mobile station of the user.

Ex. 1004, 9:26-32 (emphasis added). That paragraph is the first and only disclosure of *Sormunen*’s “PIN” (the identified “token”). To the extent that passage discloses a request for *Sormunen*’s “PIN” (the identified “token”), that passage in *Sormunen*

still fails to disclose that the request for the “PIN” (the identified “token”) is received over a “cell phone network” and via *Sormunen*’s “mobile terminal” (the identified “personal communication device”), as claim element [1.c] requires. To the contrary, because *Sormunen* discloses “when the charge card is being ordered, the number of the . . . mobile station can be given” (Ex. 1004, 9:28-29) (emphasis added), that disclosure indicates that the request for *Sormunen*’s “PIN” is not being received over a “cell phone network” or via *Sormunen*’s “mobile terminal,” but rather over some other network and via some other device (e.g., *Sormunen*’s “access terminal 8”). Otherwise, if the request for *Sormunen*’s “PIN” was being received over a “cell phone network” and via *Sormunen*’s “mobile terminal,” the phone number of *Sormunen*’s “mobile terminal” would already be known to the component that receives the request for *Sormunen*’s “PIN,” and there would be no need for the user to “give[]” the phone number. This is also consistent with other disclosures in *Sormunen*, where the “mobile terminal” is not used to request data. *See, e.g.*, Ex. 1004, 6:17-18 (“Thus the mobile station is not needed in the data inquiry phase.”).

Further, it only makes sense that *Sormunen*’s “PIN” for a bank/credit card (the identified “token”) is not requested via *Sormunen*’s “mobile terminal” (the identified “personal communication device”). *Sormunen* stresses the importance of not letting the PIN “fall[] into the wrong hands.” Ex. 1004, 9:33-34. A person often carries both their credit card and their cellphone on their person. If both items are misplaced

or stolen, the “PIN” could be requested using the cellphone, and the thief could use the stolen cellphone to obtain a new PIN for the stolen credit card, and gain access to the victim’s money. Accordingly, *Sormunen* does not teach or suggest claim element [1.c].

Perlman does not cure the deficiencies of *Sormunen*, and the Petition does not contend otherwise. *See* Pet., pp. 32-34. In view of the above, the combination of *Sormunen* and *Perlman* fails to teach or suggest claim element [1.c], and thus fails to render claim 1 obvious.

- ii. [1.d] “generating a new password . . . based at least upon the token and a passcode . . .”

Claim element [1.d] recites “generating a new password for said first secure computer network based at least upon the token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user.” Petitioner mapped *Sormunen*’s “password” and “PIN” to the claimed “passcode” and “token,” respectively. *See* Pet., pp. 34 (“A POSA would have found it obvious for the new password to be combination of the known password (passcode) and the PIN (token)”) (emphasis added), 35 (“A POSA would have understood that this initial password teaches the claimed ‘passcode’”). Petitioner concedes, however, that *Sormunen* does not disclose “generating a new password . . . based at least upon the token and a passcode,” as claim element [1.d] requires. *See* Pet., pp. 35-36. Instead,

Petitioner proposes modifying the system in *Sormunen* such that it “generat[es] a new password” by concatenating *Sormunen*’s “password” (the identified “passcode”) and “PIN” (the identified “token”), as allegedly disclosed by *Perlman*. See Pet., pp. 35-36. The motivation for the modification to *Sormunen* is “a more secure password.” Pet., p. 35. See also *id.* at 22 (“A POSA would have been motivated to modify *Sormunen* with the teachings of *Perlman* to allow for greater security and ease of use.”), 34 (“a POSA would appreciate that a password and a PIN could be used together for greater security”). Petitioner’s obviousness analysis is flawed for multiple reasons.

Petitioner analogizes *Perlman*’s “character string” (from the token) and the existing secret value (from the user) with *Sormunen*’s “PIN” and “password,” respectively. Then, Petitioner proposes combining *Sormunen*’s “PIN” and “password” like *Perlman* combines its “character string” (from the token) and the existing secret value (from the user). See Pet., pp. 36 (“A POSA would have appreciated that *Perlman* teaches concatenating a known secret character string [(i.e., existing secret value from the user)] with a generated character string provided through a token. A POSA would have appreciated that the resulting character string could be used more securely as a password than the original known secret character string. Thus, a POSA would have been motivated to combine the teachings of *Perlman* with *Sormunen*.”) (citations omitted), 34 (“*Perlman* teaches using a

character string generated by an authentication token to augment an existing character string. Thus, a POSA would have appreciated that Perlman teaches augmenting a known character string using a requested character string unknown to the user, at least at that point (token).”).

But the Petition conveniently glosses over the fact that *Sormunen*’s “PIN” is for a bank/credit card. *See* Ex. 1004, 9:26-28 (“the present invention can be applied also for obtaining a personal identity number (PIN) of bank and credit cards and corresponding charge cards”) (emphasis added). Accordingly, *Sormunen*’s “PIN” is something that the user would input at a merchant’s point-of-sale terminal or at an automated teller machine (ATM). By virtue of being a PIN for a bank/credit card, *Sormunen*’s “PIN” is reused multiple times (i.e., multiple visits to ATMs, multiple visits to merchants) over months, if not years. In fact, *Sormunen* only contemplates changing the “PIN” when “it is suspected that the [PIN] has fallen into the wrong hands.” Ex. 1004, 9:35-10:2. That is in stark contrast to *Perlman*’s “character string,” which, as discussed above, can only be used for a single authentication attempt.

Accordingly, even if *Sormunen*’s “password” is combined with *Sormunen*’s “PIN,” *Sormunen*’s modified system will not have the enhanced or “more secure” password found in *Perlman* due to the long life of *Sormunen*’s “PIN.” Specifically, in *Sormunen*’s modified system, the user will logon multiple times, over the course

of months or longer, using the concatenation of the same “password” and the same “PIN.” A hacker only needs to intercept that transmitted concatenation of the “password” and the “PIN” once before the hacker too can access the system. Thus, there is no motivation to modify *Sormunen* based on *Perlman*, as proposed by Petitioner.

Further, according to the Petition, “a POSA would appreciate that a password and a PIN could be used together for greater security. For example, they could be used together to address the known problem of a third party obtaining (e.g., guessing, intercepting) one item of user specific authentication data.” Pet., p. 34 (citations omitted). But in *Sormunen*’s system, both before and after the proposed modification based on *Perlman*, *Sormunen*’s “password” and “PIN” are still transmitted separately to the user’s “mobile terminal.” See Ex. 1004, 6:35-7:7, 9:30-32. So the problem of third-party interception of “one item of user specific authentication data” is not resolved by Petitioner’s proposed modification of *Sormunen* based on *Perlman*. Additionally, as discussed above, it is not necessary for a hacker to determine *Sormunen*’s “password” separately from *Sormunen*’s “PIN” to gain access. Following the proposed modifications to *Sormunen*, it is only necessary for a hacker to intercept the concatenation of *Sormunen*’s “PIN” and “password” to gain access. Accordingly, Petitioner’s proposed modification to

Sormunen still does not solve the identified problems. Thus, there is no motivation to combine *Sormunen* and *Perlman*.

Further, *Perlman* cautions against using a “character string” that is “too short (such as only 2^{32} possible values)” due to potential “eavesdroppers.” Ex. 1005, 6:52-57. In contrast, *Sormunen*’s “PIN” for a credit/bank card is likely only four decimal digits so the user can easily remember it. Four decimal digits is 10^4 possible values (10,000 possible values), which is orders of magnitude less than the 2^{32} possible values (4,294,967,296 possible values) in a two-character string. Thus, *Perlman* teaches that *Sormunen*’s “PIN” is too short for use as a “character string.” Accordingly, *Perlman* teaches away from Petitioner’s proposed modification of *Sormunen* based on *Perlman* (i.e., utilizing *Sormunen*’s “PIN” like *Perlman*’s “character string” from the token).

Still referring to *Perlman*, the “authentication token” is similar to RSA’s SecurID product disclosed in the ’658 Patent. See Ex. 1001, 1:44-59. Both *Perlman*’s “authentication token” and RSA’s SecurID product are additional devices (i.e., not the user’s cellphone, not the user’s pager) that the user must carry with him/her and that locally generate one-time access codes based on time, without receiving the token. Compare Ex. 1005, 5:46-64, 6:20-38 with Ex. 1001, 1:44-59. But the ’658 Patent expressly discloses the claimed invention is designed to operate with the user’s personal communication device to save the user from having to carry

around yet another device like RSA's SecurID product, and thus *Perlman's* "authentication token." *See* Ex. 1001, 1:56-59 ("It would be advantageous if the benefits of the SecurID system could be achieved using a device that many users already carry—a personal communication device such as a mobile phone or a pager.") (emphasis added). Accordingly, *Perlman* with its necessary "authentication token" teaches away from the claimed invention and cannot render the claimed invention obvious. "Obviousness may be defeated if the prior art . . . teaches away from the invention. A reference teaches away when a person of ordinary skill, upon reading the reference . . . would be led in a direction divergent from the path that was taken in the claim." *Meiresonne v. Google, Inc.*, 849 F.3d 1379, 1382 (Fed. Cir. 2017) (cleaned up). The Petition is effectively taking the same prior art (i.e., RSA's SecurID product) and recasting it through impermissible hindsight.

Further, *Sormunen's* system (1) receives a "request message" for a "password," (2) transmits the "password" in a "reply message" to the "mobile terminal 3" of the user, and then (3) receives the "password" from an "access terminal 8" operated by the user. *See* Ex. 1004, 6:2-7:12, Fig. 2. For the user to be authenticated, the "password" received from the "access terminal 8" must match the "password" sent in the "reply message" to the "mobile terminal." *See* Ex. 1004, 7:9-20. Those steps, and the specified ordering of those steps, are necessary for *Sormunen's* system to work. Accordingly, those steps define *Sormunen's* principle

of operation. Any change/addition to those fundamental steps is a change in *Sormunen*'s principle of operation.

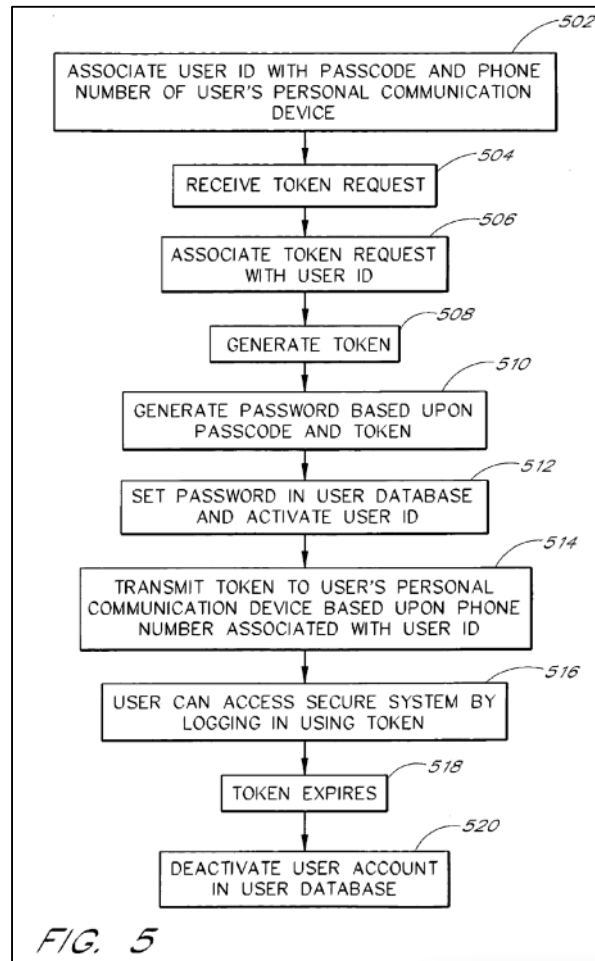
Following implementation of Petitioner's proposed modification to *Sormunen*, (a) *Sormunen*'s system must now concatenate a "PIN" for a credit/bank card with the "password," (b) the "access terminal" or "mobile terminal" must also concatenate the "PIN" for the credit/bank card with the "password," and (c) *Sormunen*'s system must receive the concatenation of the "PIN" for the credit/bank card with the "password" from the "access terminal." The user is authenticated if the concatenated value generated in (a) matches the concatenated value received in (c). Those new fundamental steps and/or modifications to *Sormunen*'s existing fundamental steps change *Sormunen*'s principle of operation, and are thus too drastic to be obvious. *See* MPEP § 2143.01 ("If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious.") (citing *In re Ratti*, 270 F.2d 810, 813 (CCPA 1959)).

In view of the above, Petitioner fails to show that the combination of *Sormunen* and *Perlman* teaches or suggests claim element [1.d], and thus fails to show that the combination of *Sormunen* and *Perlman* renders claim 1 obvious.

iii. [1.f] “activating access the user account on the first secure computer network”

Claim element [1.f] recites “activating access the user account on the first secure computer network.” According to Petitioner, “Sormunen disclose[s] this step.” Pet., p. 38 (emphasis added). Patent Owner disagrees.

Based on both logic and the express ordering of the limitations in claim 1, claim element [1.f] is executed after the claimed “password” is generated “based at least upon a token and a passcode,” and thus claim element [1.f] is executed after the claimed “token” is generated. *Compare* claim element [1.f] *with* claim element [1.d]. Claim element [1.f] is also executed before “transmitting the token to the personal communication device,” and thus before “receiving the password from the user.” *Compare* claim element [1.f] *with* claim elements [1.g] and [1.h]. That interpretation is also consistent with the specification of the ’658 Patent. For example, in Figure 5, the token is generated first (step 508), the password is generated (step 510) after the token is generated, and the account is activated (step 512) after the password is generated:



Ex. 1001, Fig. 5. As also shown in Fig. 5, the account is activated (step 512) before both transmitting the token to the personal communication device (step 514) and receiving the password from the user (step 516).

As discussed above, Petitioner mapped *Sormunen's* “PIN” for a credit/bank card to the claimed “token.” *See* Pet. at 34. Although not entirely clear, Petitioner appears to have mapped a time point “almost immediately” following transmission of the “short message” that includes “a password request and possibly also a subscription request for a new user” to the claimed “activating access [to] the user

account.” *See* Pet. at 38 (citing Ex. 1004, 5:38-6:2, 5:11-16). But Petitioner provides no evidence that the time point (the identified “activating access [to] the user account”) is after generation of *Sormunen*’s “PIN” for the bank/credit card (the identified “token”), as claim 1 requires. Petitioner also fails to provide evidence that the time point (the identified “activating access [to] the user account”) is before transmission of *Sormunen*’s “PIN” for the credit/bank card (the identified “token”) to *Sormunen*’s “mobile terminal” (the identified “personal communication device”), as claim 1 also requires.

Further, as discussed above, *Sormunen* fails to disclose generating a password based on *Sormunen*’s “PIN” for the bank/credit card (the identified “token”), as claim 1 requires. Accordingly, *Sormunen* fails to disclose generating the claimed “password” and thus cannot disclose executing claim element [1.f] after generating the claimed “password,” as claim 1 requires.

To the extent Petitioner is mapping the “using of the service” in *Sormunen* to claim element [1.f] (*see* Pet., p. 38), this too fails. As discussed above, claim element [1.f] is executed before “receiving the password from the user.” If the user is “using [] the service” in *Sormunen*, the user must necessarily have already provided the correct password. In other words, the “using of the service” in *Sormunen* (the identified “activating access [to] the user account”) necessarily takes place after receiving the password from the user. This is contrary to what claim 1 requires.

In view of the above, *Sormunen* fails to disclose claim element [1.f]. Again, Petitioner does not rely on *Perlman* to meet the requirements of claim element [1.f]. See Pet., p. 38 (“*Sormunen* disclose[s] this step”). Accordingly, the Petition fails to show that the combination of *Sormunen* and *Perlman* teaches or suggests claim element [1.f], and thus fails to show that the combination of *Sormunen* and *Perlman* renders claim 1 obvious.

iv. [1.h] “receiving the password from the user via the first secure computer network”

Claim element [1.h] recites “receiving the password from the user via the first secure computer network.” According to Petitioner, claim element [1.h] is disclosed by *Sormunen*. See Pet., p. 39 (“*Sormunen* discloses receiving the password from the user via the first secure computer network”) (emphasis added). But the claimed “password” is based on a “token” and a “passcode.” Compare claim element [1.h] with claim element [1.d]. As Petitioner concedes, *Sormunen*’s “password” is not based on a “token” and a “passcode.” See Pet., pp. 35-36. See also Ex. 1004, 6:22-24. Accordingly, *Sormunen* fails to disclose the claimed “password” and thus cannot disclose claim element [1.h].

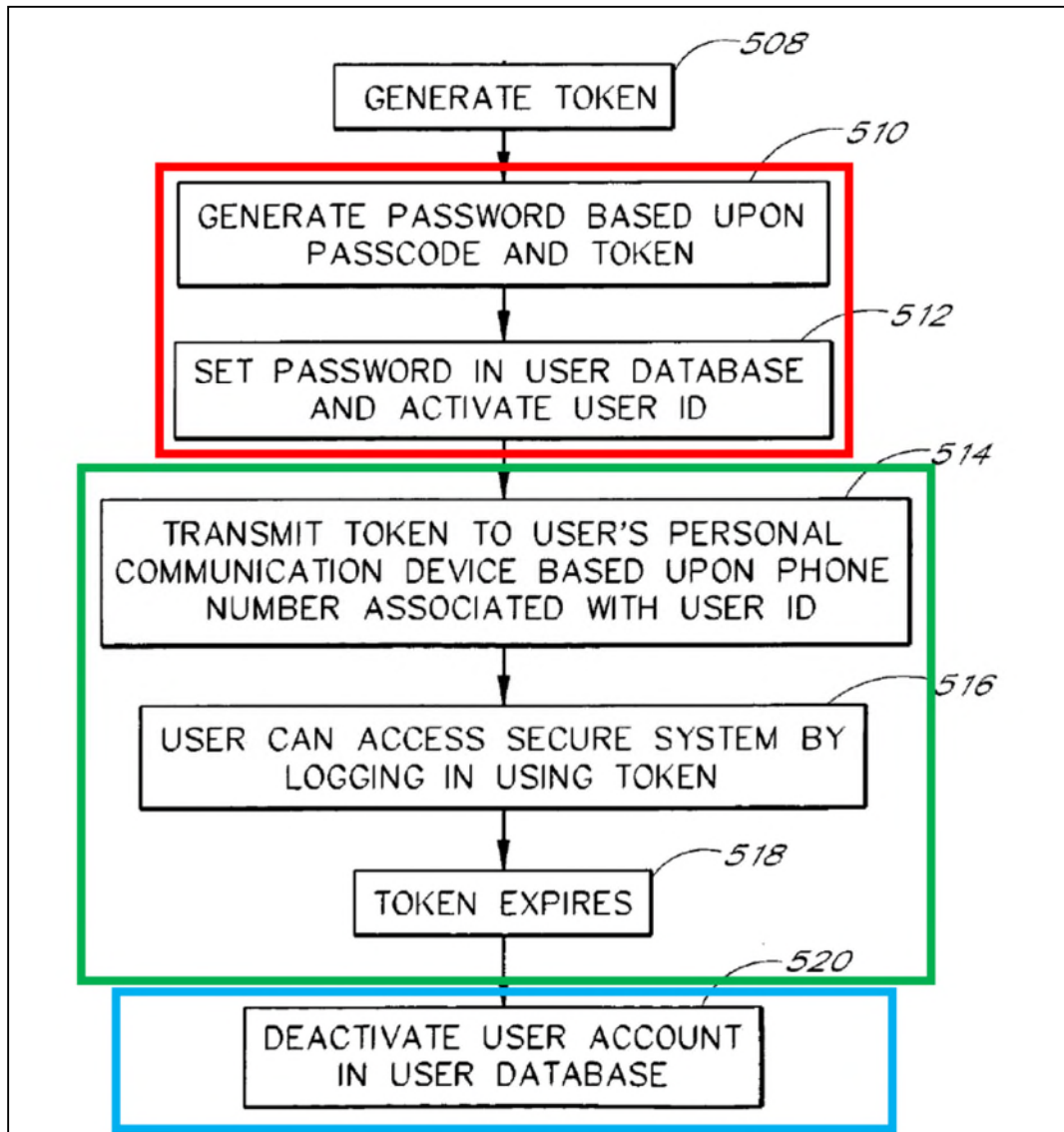
To the extent the Petition is relying on the combination of *Sormunen* and *Perlman* to meet claim element [1.h], Patent Owner asserts there is no motivation to

combine *Sormunen* and *Perlman* for all the reasons discussed above in reference to claim element [1.d].

In view of the above, Petitioner fails to show that *Sormunen* alone or the combination of *Sormunen* and *Perlman* teaches or suggests claim element [1.h], and thus fails to show that the combination of *Sormunen* and *Perlman* renders claim 1 obvious.

- v. [1.i] “deactivating access to the user account . . . within a predetermined amount of time after said activating . . .”

Claim element [1.i] recites “deactivating access to the user account on the first secure computer network within a predetermined amount of time after said activating, such that said user account is not accessible through any password, via said first secure computer network.” The “said activating” refers to “activating access [to] the user account on the first secure network.” *Compare* claim element [1.i] *with* claim element [1.f]. The language of the claim is unequivocal: the “predetermined amount of time” starts “after said activating” and ends upon “deactivating access to the user account.” The same process is depicted, for example, in Figure 5, which is reproduced in pertinent part below:



Ex. 1001, Fig. 5 (excerpted and annotated). Activating account access in response to generation of the new “password” is depicted in steps 510 and 512 of Figure 5 (as highlighted in red in Figure 5). *See id.* at 9:28-43, Fig. 5. Deactivation of the account occurs in step 520 (as highlighted in blue in Figure 5). *See id.* at 9:61-64, Fig. 5. The “predetermined amount of time” is the time period between those two events

(as highlighted in green in Figure 5). *See id.* at 12:41-47, Fig. 5. Petitioner's arguments fail for the following reasons.

First, Petitioner argues that *Sormunen* discloses account activation when “the user is given access” because “the password submitted through access terminal 8 matches the one in the system.” Pet., p. 40 (citing Ex. 1004, 7:9-20). Petitioner concedes that process occurs after *Sormunen*'s system receives the password from the user, unlike claim 1, which as discussed above in reference to claim element [1.f], requires that activating access to the account occur before receiving the “password” from the user. *See id.* That step in *Sormunen* (i.e., granting access because of matching passwords) is akin to step 516 in Figure 5 of the '684 Patent, which occurs after activating access, and after the “predetermined amount of time” has begun (as highlighted in green above). In the '658 Patent, the process authenticates the user (i.e., permits access) by comparing the “password” received from the user with the “password associated with the user.” *See* Ex. 1001, 7:15-17 (“the authentication module 112 then compares hashes of passwords rather than the passwords themselves to authenticate the user 108”), 9:54-59 (“The user then logs in using his user ID 152 and the password 158.”), Fig. 5. Thus, the Petition incorrectly identifies a process that occurs after *Sormunen* receives the alleged “password” from the user, unlike claim 1, which requires activating access to the account before receiving the “password” from the user.

Second, Petitioner mapped the time window when a password is valid (hereinafter “password validity period”) in *Sormunen* to the claimed “predetermined amount of time.” See Pet., p. 41. But *Sormunen*’s password validity period (the identified “predetermined amount of time”) does not start after “the user is given access” because “the password submitted through access terminal 8 matches the one in the system” (the identified “said activating”), as claim 1 requires. *Sormunen*’s password validity period (the identified “predetermined amount of time”) would start when *Sormunen*’s password is generated, or at the latest, when *Sormunen*’s password is transmitted to user’s “mobile terminal.” Both events (i.e., password generation, transmission of password to user’s mobile terminal) are necessarily before “the user is given access” because “the password submitted through access terminal 8 matches the one in the system” (the identified “said activating”). This is contrary to what claim 1 requires.

In view of the above, Petitioner fails to show that the combination of *Sormunen* and *Perlman* teaches or suggests claim element [1.i], and thus fails to show that the combination of *Sormunen* and *Perlman* renders claim 1 obvious.

2. Dependent Claims 2-4

Claims 2-4 depend from and add limitations to independent claim 1. As discussed above, the combination of *Sormunen* and *Perlman* fails to render independent claim 1 unpatentable. Therefore, the combination of *Sormunen* and

Perlman fails to render dependent claims 2-4 unpatentable for at least the same reasons.

3. Independent Claim 5

The combination of *Sormunen* and *Perlman* does not render obvious independent claim 5 because the combination does not teach or suggest the following elements of the claim.

- i. [5.d] “a control module . . . configured to create a new password based at least upon a token and a passcode . . .”

Claim element [5.d] recites “a control module executed on the computer processor configured to create a new password based at least upon a token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user, the control module further configured to set a password associated with the user to be the new password.” The Petition relies on and refers back to claim element [1.d] to argue that claim element [5.d] is obvious in view of *Sormunen* and *Perlman*. Pet., p. 46. Accordingly, the combination of *Sormunen* and *Perlman* fails to teach or suggest claim element [5.d] for the same reasons above with respect to claim element [1.d].

For at least these reasons, the combination of *Sormunen* and *Perlman* fails to teach or suggest claim element [5.d]. Accordingly, the combination of *Sormunen* and *Perlman* fails to render independent claim 5 unpatentable.

- ii. [5.f] “an authentication module configured to receive the password from the user . . . wherein the authentication module activates access to the account in response to the password and deactivates the account within a predetermined amount of time after activating the account . . .”

Claim element [5.f] recites “an authentication module configured to receive the password from the user through a secure computer network, said secure computer network being different from the cell phone network, wherein the user has an account on the secure computer network, wherein the authentication module activates access to the account in response to the password and deactivates the account within a predetermined amount of time after activating the account, such that said account is not accessible through any password via the secure computer network.” The Petition relies on and refers back to claim elements [1.f], [1.h], and [1.i] to argue that claim element [5.f] is obvious in view of *Sormunen* and *Perlman*. Pet., p. 47. Accordingly, the combination of *Sormunen* and *Perlman* fails to teach or suggest claim element [5.f] for the same reasons above with respect to claim elements [1.f], [1.h], and [1.i].

Further, the plain language of claim element [5.f] requires activation of account access in response to generation of the claimed “new password.” The relevant portions of claim 5 are reproduced below:

a control module executed on the computer processor configured to create a new password based at least upon a token and a passcode, wherein the

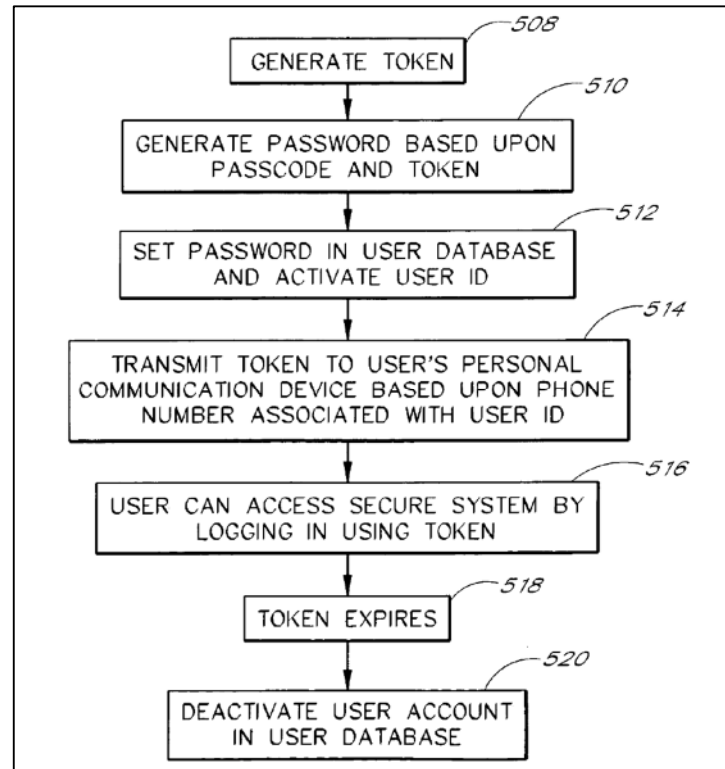
token is not known to the user and wherein the passcode is known to the user, the control module further configured to set a password associated with the user to be the new password;

* * * * *

an authentication module configured to receive the password from the user through a secure computer network, said secure computer network being different from the cell phone network, wherein the user has an account on the secure computer network, wherein the authentication module activates access to the account in response to the password and deactivates the account within a predetermined amount of time after activating the account, such that said account is not accessible through any password via the secure computer network.

Ex. 1001 at 12:27-47 (emphasis added). The “control module” creates a “new password.” Then it sets a “password” to be the “new password” that was created by the “control module.” *Id.* at 12:27-33. The “authentication module” claim element recites “the password” several times. *See id.* at 12:37-47. The “a password” term recited in the “control module” claim element provides the antecedent basis for “the password” term in the “authentication module” claim element. *See id.* at 12:27-47. Thus, when the claim recites “wherein the authentication module activates access to the account in response to the password,” it is referring to the “a password” that is introduced in the “control module” claim element. *See id.* So it follows, from the plain language of the claim, that creation of that password is a prerequisite to the “authentication module activat[ing] access to the account in response to the password.” *See id.*

That same process is depicted, for example, in Figure 5 of the '658 Patent, which is reproduced in pertinent part below:



Ex. 1001, Fig. 5. The password is generated in step 510, which causes activation of access to the user's account in step 512. *See id.* Patent Owner's interpretation of claim 5 is also consistent with the Claim Construction Order issued by the United States District Court for the Eastern District of Texas on October 31:

For the foregoing reasons, the Court construes “activates access to the account in response to the password” as “activates access to the account in response to the creation of the password.”

Ex. 2002, p. 13. The Board is required to apply the same claim-construction standard as in Federal district court. *See* 37 C.F.R. § 42.100(b).

Petitioner argues that *Sormunen* discloses account activation when “the user is given access” because “the password submitted through access terminal 8 matches the one in the system.” Pet., p. 40 (citing Ex. 1004, 7:9-20). Petitioner concedes that process occurs after *Sormunen*’s system receives the password from the user, unlike claim 5, which requires that the “authentication module” activates access to the account in response to creation of the new “password,” not in response to receiving the “password” from the user, after the token is sent to the user. *See id.* That step in *Sormunen* (i.e., granting access because of matching passwords) is akin to step 516 in Figure 5 of the ’684 Patent, which occurs after activation of access, and after the “predetermined period of time” has begun. In the ’658 Patent, the “authentication module” authenticates the user (i.e., permits access) by comparing the “password” received from the user with the “password associated with the user.” *See* Ex. 1001, 7:15-17 (“the authentication module 112 then compares hashes of passwords rather than the passwords themselves to authenticate the user 108”), 9:54-59 (“The user then logs in using his user ID 152 and the password 158.”), Fig. 5.

Thus, the Petition incorrectly identifies a process that occurs after *Sormunen* receives the alleged “password” from the user, unlike claim 5, which requires that the “authentication module” activates access to the account in response to creation of the new “password,” not in response to receiving the “password” from the user.

For at least these reasons, the combination of *Sormunen* and *Perlman* fails to teach or suggest claim element [5.f]. Accordingly, the combination of *Sormunen* and *Perlman* fails to render independent claim 5 unpatentable.

4. Dependent Claims 6 and 7

Claims 6 and 7 depend from and add limitations to independent claim 5. As discussed above, the combination of *Sormunen* and *Perlman* fails to render independent claim 5 unpatentable. Therefore, the combination of *Sormunen* and *Perlman* fails to render dependent claims 6 and 7 unpatentable for at least the same reasons.

IV. THE BOARD SHOULD EXERCISE ITS DISCRETION TO DENY THE PETITION.

The Petition constitutes the third bite of the apple in an attempt to invalidate the claims of the '658 Patent. Several district court defendants filed the first petition with the following grounds of unpatentability:

The Challenged Claims are unpatentable under the following grounds:			
Ground	Claims	Reference(s)	Basis
1	1-3, 5-7	Guthrie, Sormunen	§ 103
2	1-3, 5-7	Kato, Guthrie	§ 103

Bank of America, N.A., et al. v. Dynapass IP Holdings LLC, IPR2023-00367, Paper No. 1, p. 1 (P.T.A.B. Jan. 3, 2023). The Board denied institution on July 18, 2023.

Several days later, Unified Patents filed second with the following grounds of unpatentability:

The grounds for challenge include:		
Ground	References	Challenged Claims
1	<i>Veneklase</i> in view of <i>Jonsson</i>	5
2	<i>Kew</i> in view of <i>Sormunen</i>	1, 3-6

Unified Patents, LLC v. Dynapass IP Holdings LLC, IPR2023-00425, Paper No. 1, p. 2 (P.T.A.B. Jan. 6, 2023). That petition was instituted on July 18, 2023.

Petitioner was served with a patent-infringement complaint on February 22, 2023, less than two months after the defendants filed IPR2023-00367 on January 3, 2023. Ex. 2003. The institution decisions in IPR2023-00367 and IPR2023-00425

issued nearly five months after Petitioner was served with the complaint. But Petitioner waited an additional two months after those decisions—a total of seven months after service of the complaint—to take a third bite at the apple,² filing the instant Petition on September 28, 2023. Despite Petitioner’s delay, and having two months to review the institution decisions in IPR2023-00367 and IPR2023-00425 before filing the instant Petition, Petitioner’s grounds for unpatentability do nothing more than retread over familiar ground:

Ground	Claims	Reference(s)
1	1–7	Sormunen in view of Perlman

Pet., p. 15.

The *Sormunen* reference has been asserted in all of the previously filed petitions for *inter partes* review of the ’658 Patent, including IPR2023-00367, which was denied. And Petitioner concedes that *Perlman* was considered by the Patent Office during prosecution of the ’658 Patent. *See* Pet., p. 49 (“While Perlman was cited as relevant in an international search report and information disclosure statement. . . .”); *see also* Ex. 1001. Because the Petition does nothing more than

² JPMorgan Chase Bank, N.A. filed a petition for *inter partes* review on August 16, 2023, before the instant Petition, but that petition “is substantively identical to the petition in the Unified Patents IPR—challenging the same claims of the ’658 Patent on the same grounds while relying on the same prior art, arguments, and evidence.” *JPMorgan Chase Bank, N.A. v. Dynapass IP Holdings LLC*, IPR2023-01331, Paper No. 2 p. 2 (P.T.A.B. August 16, 2023).

reassert prior art and arguments that have already been considered by the Patent Office, and the Petition was filed with the benefit of using the institution decisions in IPR2023-00367 and IPR2023-00425 as roadmaps, the Board should exercise its discretion to deny the Petition for at least the following two reasons.

A. The Board Should Exercise Its Discretion to Deny the Petition Under 35 U.S.C. § 314(a).

The Board has discretion as to whether to institute *inter partes* review. *See* 35 U.S.C. § 314(a); *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2140 (2016) (“[T]he agency’s decision to deny a petition is a matter committed to the Patent Office’s discretion.”). The Petition should be denied under 35 U.S.C. § 314(a) in view of the *General Plastic* factors.

In *General Plastic*, the Board recognized “the potential for abuse of the review process by repeated attacks on patents.” *General Plastic Indus. Co. v. Canon Kabushiki Kaisha*, IPR2016-01357, Paper 19 at 17 (P.T.A.B. Sept. 6, 2017) (precedential). To mitigate such abuse, the Board identified seven factors that it considers in determining whether to institute decision of a subsequent petition:

1. whether the same petitioner previously filed a petition directed to the same claims of the same patent;
2. whether at the time of filing of the first petition the petitioner knew of the prior art asserted in the second petition or should have known of it;

3. whether at the time of filing of the second petition the petitioner already received the patent owner's preliminary response to the first petition or received the Board's decision on whether to institute review in the first petition;
4. the length of time that elapsed between the time the petitioner learned of the prior art asserted in the second petition and the filing of the second petition;
5. whether the petitioner provides adequate explanation for the time elapsed between the filings of multiple petitions directed to the same claims of the same patent;
6. the finite resources of the Board; and
7. the requirement under 35 U.S.C. § 316(a)(11) to issue a final determination not later than 1 year after the date on which the Director notices institution of review.

Id., Paper 19 at 16. In the present case, the *General Plastic* factors overwhelmingly favor denying institution.

1. General Plastic Factor One

Under the first *General Plastic* factor, the Board considers “whether the same petitioner filed a petition directed to the same claims of the same patent.” *General Plastic*, Paper 19 at 16. In *Valve Corporation*, the Board clarified that the

“application of the *General Plastic* factors is not limited solely to instances when multiple petitions are filed by the same petitioner. Rather, when different petitioners challenge the same patent, [the Board considers] any relationship between those petitioners when weighing the *General Plastic* factors.” *Valve Corporation v. Electronic Scripting Products, Inc.*, IPR2019-00062, Paper 11 at 9 (P.T.A.B. April 2, 2019) (precedential) (emphasis added); *see also NetApp Inc. v. Realtime Data LLC*, IPR2017- 01195, Paper 9 at 10 (P.T.A.B. Oct. 12, 2017) (“[T]he General Plastic factors provide a useful framework for analyzing the facts and circumstances present in this case, in which a different petitioner filed a petition challenging a patent that had been challenged already by previous petitions.” (emphasis added)). In *Ericsson Inc. v. Uniloc*, the Board weighed the first *General Plastic* factor against institution because “[t]he instant Petitioner’s decision to use the prior petitions as a roadmap for its own petition ties the interests of all the petitioners together.” *Ericsson Inc. v. Uniloc 2017, LLC*, IPR2019-01550, Paper 8 at 12 (Mar. 17, 2020).

The first *General Plastic* factor weights heavily in favor of denying institution because the instant Petition was filed with the benefit of using the institution decisions in IPR2023-00367 and IPR2023-00425 as roadmaps. The IPR2023-00367 defendants previously filed a petition for *inter partes* review of claims 1-3 and 5-7 of the ’658 Patent. *Bank of America, N.A., et al. v. Dynapass IP Holdings LLC*, IPR2023-00367, Paper No. 1, p. 1 (P.T.A.B. Jan. 3, 2023). Several days later,

Unified Patents similarly filed a petition for *inter partes* review of claims 1 and 3–6 of the '658 Patent. *Unified Patents, LLC v. Dynapass IP Holdings LLC*, IPR2023-00425, Paper No. 1, p. (P.T.A.B. Jan. 6, 2023). This Petition and the petitions in IPR2023-00367 and IPR2023-00425 challenge all but one of the exact same claims. *Compare* Pet., p. 1 (challenging claims 1–7), *with Bank of America, N.A., et al. v. Dynapass IP Holdings LLC et al.*, Paper 1 at 1 (challenging claims 1–3 and 5–7), *and Unified Patents, LLC v. Dynapass IP Holdings LLC*, IPR2023-00425, Paper 1 at 1 (challenging claims 1 and 3–6). Petitioner's decision to use the IPR2023-00367 and IPR2023-00425 petitions as a roadmap for its own Petition "ties the interest of all the petitioners together." *See Ericsson Inc. v. Uniloc 2017, LLC*, IPR2019-01550, Paper 8 at 12 ("[t]he instant Petitioner's decision to use the prior petitions as a roadmap for its own petition ties the interests of all the petitioners together.").

There is also a significant relationship between the IPR2023-00367 defendants and Petitioner because both were sued for infringement of the '658 Patent in the same district court. *Compare Dynapass IP Holdings, LLC v. Bank of America Corporation*, No. 2:22-cv-000210 (E.D. Tex. June 17, 2022), *with Dynapass IP Holdings, LLC v. Experian Information Services, Inc.*, No. 2:23-cv-00066 (E.D. Tex. Feb. 20, 2023). Petitioner even admits that the patent infringement lawsuits against the IPR2023-00367 defendants are related cases. Pet., pp. 53–55.

Accordingly, there is a significant relationship between the IPR2023-00367 defendants, Unified Patents, and Petitioner with respect to Patent Owner’s assertion of the ’658 Patent. The overlap in the challenged claims and the significant relationship between the IPR2023-00367 defendants, Unified Patents (IPR2023-00425), and Petitioner favor denying institution.

2. General Plastic Factor Two

Under the second *General Plastic* factor, the Board considers “whether at the time of filing of the first petition the petitioner knew of the prior art asserted in the second petition or should have known of it.” *General Plastic*, Paper 19 at 16. Here, Petitioner knew or should have known of the prior art references in the Petition—*Sormunen* and *Perlman*—when the IPR2023-00367 defendants filed their petition. The institution decisions in IPR2023-00367 and IPR2023-00425 issued nearly five months after Petitioner was served with the complaint. Petitioner then waited an additional two months after the institution decisions in IPR2023-00367 and IPR2023-00425 to file the instant Petition. The *Sormunen* reference has been asserted in all of the previously filed petitions for *inter partes* review of the ’658 Patent. Petitioner concedes that *Perlman* was considered by the Patent Office during prosecution of the ’658 Patent. *See* Pet., p. 49 (“While Perlman was cited as relevant in an international search report and information disclosure statement. . . .”); *see also* Ex. 1001. As discussed above, both Petitioner and the IPR2023-00367 defendants

were sued for infringement of the '658 Patent in the same district court. Petitioner even admits it was aware of the infringement lawsuit against the IPR2023-00367 defendants. Pet., pp. 53–55 (listing related matters). Accordingly, Petitioner and the IPR2023-00367 defendants are similarly situated. Petitioner knew or should have known of the prior art references in the Petition around the time the IPR2023-00367 petition was filed because *Sormunen* was also relied upon by Petitioner, and *Perlman* was previously considered by the Patent Office during prosecution.

Further, in *Apple Inc. v. Uniloc 2017 LLC*, the Board found that this factor favored denying institution because Apple failed to “set forth facts or offer an explanation concerning its knowledge, at the time it filed the first petition, of the prior art asserted in the [later petition].” *Apple Inc. v. Uniloc 2017 LLC*, IPR2020-00854, Paper 9 at 9 (P.T.A.B. Oct. 28, 2020) (precedential). In the present case, like in *Apple Inc. v. Uniloc 2017 LLC*, Petitioner provides no explanation as to when it knew about the prior art references asserted in the later petition. This factor favors denying institution.

3. General Plastic Factor Three

Under the third *General Plastic* factor, the Board considers “whether at the time of filing of the second petition the petitioner already received the patent owner’s preliminary response to the first petition or received the Board’s decision on whether to institute review in the first petition.” *General Plastic*, Paper 19 at 16.

The patent owner's preliminary response in IPR2023-00425 was filed on April 25, 2023, and the Board instituted the IPR on July 18, 2023. The patent owner's preliminary response in IPR2023-00367 was filed on April 27, 2023, and the Board denied institution on July 18, 2023. The Petition was filed several months later, on September 28, 2023. Accordingly, Petitioner had access to Patent Owner's preliminary responses and the Board's decisions well before filing the Petition and thus would have been aware of Patent Owner's and the Board's arguments and positions. This factor favors denying institution.

4. *General Plastic* Factors Four and Five

Under the fourth and fifth *General Plastic* factors, the Board considers “the length of time that elapsed between the time the petitioner learned of the prior art asserted in the second petition and the filing of the second petition” and “whether the petitioner provides adequate explanation for the time elapsed between the filings of multiple petitions directed to the same claims of the same patent,” respectively. *General Plastic*, Paper 19 at 16. Petitioner knew or should have known about the prior art asserted in the Petition (*Sormunen* and *Perlman*) shortly after being served with the complaint (i.e., February 22, 2023). Petitioner was served the complaint less than two months after the defendants filed IPR2023-00367 on January 3, 2023. Ex. 2003. The institution decisions in IPR2023-00367 and IPR2023-00425 issued nearly five months after Petitioner was served with the complaint. Petitioner then

waited an additional two months after those decisions—a total of seven months after service of the complaint—to take a third bite at the apple, filing the instant Petition on September 28, 2023. As discussed above, the *Sormunen* reference has been asserted in all of the previously filed petitions for *inter partes* review of the '658 Patent. Petitioner also concedes that *Perlman* was considered by the Patent Office during prosecution of the '658 Patent. *See* Pet., p. 49.

Accordingly, Petitioner waited approximately seven months to file the Petition after learning about the prior art. Further, the Petition provides no explanation for this seven-month delay. In *Valve Corp. v. Electronic Scripting Products, Inc.*, the Board found that a five-month delay was sufficient to favor denying institution. *Valve Corp. v. Electronic Scripting Products, Inc.*, IPR2019-00064, Paper 10 at 15 (P.T.A.B. May 1, 2019) (precedential) (“The fact that Valve waited five months after HTC’s petition to file the Petition in this case favors denying institution.”). These factors favor denying institution.

5. General Plastic Factor Six and Seven

Under the sixth and seventh *General Plastic* factors, the Board considers “the finite resources of the Board” and “the requirement under 35 U.S.C. § 316(a)(11) to issue a final determination not later than 1 year after the date on which the Director notices institution of review,” respectively. *General Plastic*, Paper 19 at 16. The sixth and seventh factors are efficiency considerations. *Id.* at 16-17.

The instant Petition uses the institution decisions in IPR2023-00367 and IPR2023-00425 as roadmaps, presenting prior art and arguments that have already been considered by the Patent Office. The overlap in the challenged claims and the significant relationship between the IPR2023-00367 defendants, Unified Patents, and Petitioner favors denying institution because this virtually identical Petition would be redundant and a waste of the Board's finite resources. *See Valve Corporation v. Electronic Scripting Products, Inc.*, IPR2019-00062, Paper 11 at 15 (P.T.A.B. April 2, 2019) (precedential) ("Here, [Petitioner] waited until after the institution decision[s] in the [IPR2023-00367 and IPR2023-00425] IPR[s], and then filed . . . [an] additional petition[.]. These serial and repetitive attacks implicate the efficiency concerns underpinning *General Plastic*, and, thus, favor denying institution."). Thus, the sixth and seventh *General Plastic* factors therefore favor denying institution.

In view of the above, the *General Plastic* factors overwhelmingly favor denying institution. Accordingly, the Petition should be denied.

B. The Board Should Exercise Its Discretion to Deny the Petition Under 35 U.S.C. § 325(d).

The Patent Office evaluates Section 325(d) using a "two-part framework: (1) whether the same or substantially the same art previously was presented to the Office or whether the same or substantially the same arguments previously were presented

to the Office; and (2) if either condition of first part of the framework is satisfied, whether the petitioner has demonstrated that the Office erred in a manner material to the patentability of challenged claims.” *Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6 at 8-9 (P.T.A.B. Feb. 13, 2020) (precedential).

1. The First Part of the Framework is Satisfied by Every Reference Asserted in the Petition.

The first part of the framework is satisfied because *Sormunen* and *Perlman* were previously presented to the Office. As discussed above, *Sormunen* has been asserted in all of the previously filed petitions for *inter partes* review of the ’658 Patent—including IPR2023-00367, wherein the Board considered the merits of *Sormunen* and ultimately denied institution. Similarly, Petitioner concedes that *Perlman* was considered by the Office during prosecution of the ’658 Patent. *See* Pet., p. 49 (“While Perlman was cited as relevant in an international search report and information disclosure statement. . . .”); *see also* Ex. 1001. The first part of the § 325(d) framework is therefore satisfied for every reference cited in the Petition.

2. The Second Part of the Framework is Satisfied, So Institution Should be Denied.

The second part of the framework is satisfied because Petitioner fails to allege, let alone demonstrate, that “the Office erred in a manner material to the patentability of challenged claims.” *Advanced Bionics, LLC v. MED-EL Elektromedizinische*

Geräte GmbH, IPR2019-01469, Paper 6 at 8-9 (P.T.A.B. Feb. 13, 2020) (Precedential). Petitioner has not alleged that the Board erred in its evaluation of *Sormunen*, or that the Examiner erred in his/her evaluation of *Perlman*. Pet. *passim*. To the contrary, Petitioner alleges that the claims of the '658 Patent were ultimately allowed during prosecution because “the missing teaching in the prior art was the user’s request being sent over the separate cell phone network rather than ‘over the network account connection.’” Pet., p. 11 (emphasis added). But *Perlman* is silent regarding cell or mobile networks. *Perlman passim*. Petitioner’s argument implies that it agrees with the Examiner that *Perlman* is cumulative of the art cited in the rejections during prosecution; thus, the Office did not err. Accordingly, the second part of the framework is also satisfied, and institution should be denied under 35 U.S.C. § 325(d).

V. THE PETITION SHOULD BE DENIED BECAUSE THE BOARD DOES NOT HAVE JURISDICTION OVER EXPIRED PATENTS.

In *Oil States*, the Supreme Court explained that the “decision to *grant* a patent is a matter involving public rights—specifically, the grant of a public franchise.” *Oil States Energy Servs., LLC v. Greene’s Energy Grp., LLC*, 138 S. Ct. 1365, 1373 (2018). “Specifically, patents are public franchises that the Government grants to the inventors of new and useful improvements.” *Id.* (internal quotation marks omitted). The Court explained that “Congress [has] significant latitude to assign

[the] adjudication of public rights to entities other than Article III courts.” *Id.* at 1368. In exercising its “significant latitude,” Congress grants public franchises “subject to the qualification that the PTO has the authority to reexamine—and perhaps cancel—a patent claim in an inter partes review.” *Id.* at 1368, 1374 (internal quotation marks omitted). Accordingly, so long as the public franchise exists, the Patent Office may have jurisdiction to amend and cancel the claims of the patent (e.g., via *inter partes* review).

When a patent expires, however, the public franchise ceases to exist and the franchisee (e.g., the patent owner) no longer has the right to exclude others. At most, the franchisee may be entitled to collect damages from the public franchise that formerly existed through an infringement action in district court. But because the public franchise no longer exists, the Patent Office has nothing in its authority to cancel or amend. Expiration removes the patent from the Patent Office’s jurisdiction and returns it to the sole jurisdiction of the Article III courts, which have exclusive authority to govern claims for damages. If this were not so, the Patent Office would purport to have authority to retroactively modify a public franchise that no longer exists, in a setting where the expired public franchise does not enjoy any presumption of validity and in which amendment of claims is no longer permitted.

The ’658 Patent issued in January 2006, long before the Petition was filed on September 28, 2023. With the expiration of the ’658 Patent in March 2020, the

Board ceased to have jurisdiction over the '658 Patent, and this *inter partes* review proceeding should be terminated as a result.

VI. CONCLUSION

The Petition should be denied. Petitioner has not established that the cited references render unpatentable any challenged claim of the '658 Patent. The Petition constitutes the third bite of the apple in an attempt to invalidate the claims of the '658 Patent, which warrants discretionary denial under both 35 U.S.C. § 314(a) and 35 U.S.C. § 325(d). Alternatively, the Board should deny institution because it does not have jurisdiction over expired patents.

CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. § 42.24(d), I hereby certify that the foregoing Patent Owner's Preliminary Response contains 11,192 words as measured by the word processing software used to prepare the document, excluding the cover page, signature block, and portions exempted under 37 C.F.R. § 42.24(a) or (b).

DATED: January 5, 2024

Respectfully submitted,

By: /John Wittenzellner/
John Wittenzellner
Registration No. 61,662
Counsel for Patent Owner

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 42.6, the undersigned certifies that on January 5, 2024, the foregoing document was served on counsel of record for Petitioner by filing this document through the End-to-End System, as well as via electronic mail to counsel of record for Petitioner at the following addresses: James B. Hatten (jhatten@bakerlaw.com) and Glenn D. Richeson (gricheson@bakerlaw.com).

Respectfully submitted,

By: /John Wittenzellner/
John Wittenzellner
Registration No. 61,662
Counsel for Patent Owner