

Filed on behalf of Patent Owner by:

Paper No. ____

Elisabeth H. Hunt, Reg. No. 67,336

Richard F. Giunta, Reg. No. 36,149

Marc S. Johannes, Reg. No. 64,978

WOLF, GREENFIELD & SACKS, P.C.

600 Atlantic Avenue

Boston, MA 02210

(617) 646-8000 Phone

(617) 646-8646 Fax

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ABBOTT DIABETES CARE INC.,
Petitioner,

v.

DEXCOM, INC.,
Patent Owner.

Case No. IPR2024-00797

Patent No. 10,375,222

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	'222 PATENT	8
III.	GROUND 1 FAILS	16
A.	All Challenged Claims Require an Exchange of “Information Related to Authentication”	17
B.	“Authentication” Validates That a Device Is Authorized	17
1.	The Plain and Ordinary Meaning of “Authentication”	17
2.	The Specification Uses the Term “Authentication” Consistent With Its Ordinary Meaning	20
a.	“Authentication” Validates Authorization	20
b.	Illustrative Embodiments of Authentication	21
C.	Yarger (Ex-1005) Does Not Teach Authentication	22
1.	Overview of Yarger	22
2.	Detailed Explanation of Yarger	24
D.	The Petition Fails to Establish That the Alleged Yarger-Love Combination Exchanges “Information Related to Authentication”	28
1.	Abbott Alleges That Yarger’s NFC Pairing Exchanges “Information Relating to Authentication”	29
2.	Abbott Fails to Give Meaning to the Term “Authentication”	30
3.	Abbott Fails to Establish That Yarger’s “Secret Key” Is “Information Related to Authentication”	33
a.	Yarger’s Secret Key Is Not Used for Authentication	33
b.	Abbott Fails to Establish That Yarger’s Secret Key Is “Information Related to Authentication”	34
i.	Abbott’s argument fails as a matter of claim construction	34
ii.	Abbott fails to establish that Yarger’s secret key meets Abbott’s own construction of “information related to authentication” because Yarger’s key is not “related to identification” of any device	39

iii.	Abbott’s separate assertion that determining whether the secret key was exchanged is “authentication” fails	42
c.	Conclusion—Abbott Fails to Establish That Yarger’s Secret Key is “Information Related to Authentication”	43
4.	Abbott Fails to Establish That Yarger’s “Identifying Information” Is “Information Related to Authentication”	43
a.	Yarger’s “Identifying Information” Does Not Meet Abbott’s Own Construction of “Information Related to Authentication”	44
b.	Abbott Fails to Establish That Yarger’s “Identifying Information” Is “Information Related to Authentication”	44
i.	Identifying information is not authentication information.....	45
ii.	Yarger does not perform “authenticated pairing”.....	45
5.	Abbott Fails to Establish That Yarger’s “Secret Key” and “Identifying Information” Together Are “Information Related to Authentication”	49
6.	Abbott’s Expert Testimony Cannot Save Ground 1	50
E.	Conclusion—Ground 1 fails.....	51
IV.	GROUND 2 FAILS	51
A.	Hernandez-Rosas (Ex-1007)	51
B.	Chivallier (Ex-1008).....	56
C.	Ground 2 Fails Because the Petition Does Not Establish That a POSA Would Have Combined Hernandez-Rosas in the Way the Petition Alleges.....	58
1.	Hernandez-Rosas is Immune From the Alleged Eavesdropping Risk.....	61
2.	The Petition Fails to Explain the Contemplated Workings of the Combination	66
3.	Abbott Ignores Reasons Why a POSA Would Not Have Used Chivallier’s Passive NFC Tag and NFC Reader to Exchange Hernandez-Rosas’s Authentication Information.....	68

a.	Hernandez-Rosas’s Four-Step Challenge-Response Authentication Process Is Incompatible with NFC That Chivallier Uses for Its Simple One-Step Private Key Sharing	68
b.	Using NFC to Exchange Authentication Information Would Have Eliminated Numerous Display Devices That Hernandez-Rosas Teaches Are Desirable	71
4.	Conclusion—Ground 2 Fails.....	72
V.	CONCLUSION.....	72

TABLE OF AUTHORITIES

CASES

<i>Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve, Inc.</i> , 796 F. 2d 443 (Fed. Cir. 1986)	68
<i>Bicon, Inc. v. Straumann Co.</i> , 441 F.3d 945 (Fed. Cir. 2006)	30
<i>Dell Inc. v. Acceleron, LLC</i> , 818 F.3d 1293 (Fed. Cir. 2016)	30
<i>Hewlett Packard Enterprise Co. v. K.Mizra LLC</i> , IPR2022-00843, Paper 14 (Oct. 31, 2022)	65
<i>KSR Int’l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007)	58, 64
<i>Pers. WebTechs., LLC v. Apple, Inc.</i> , 848 F.3d 987 (Fed. Cir. 2017)	66, 68
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005)	31
<i>TQ Delta, LLC v. CISCO Sys., Inc.</i> , 942 F.3d 1352 (Fed. Cir. 2019)	58, 64
<i>Truist Bank v. United Services Automobile Association</i> , Paper 15 at 25-26, IPR2023-00143 (May 16, 2023)	65
<i>Unigene Labs., Inc. v. Apotex, Inc.</i> , 655 F.3d 1352 (Fed. Cir. 2011)	58, 65
<i>W.L. Gore & Assoc., Inc. v. Garlock, Inc.</i> , 721 F.2d 1540 (Fed. Cir. 1983)	68
<i>Xerox v. Bytemark</i> , IPR2022-00624, Paper 9 (Aug. 24, 2022)	50

REGULATIONS

37 C.F.R. § 42.104(b)(3)	31
--------------------------------	----

37 C.F.R. § 42.104(b)(4).....	31, 39, 44
37 C.F.R. § 42.65(a).....	50

LISTING OF EXHIBITS

Exhibit	Description
2001	Dictionary of Computing Science, Seventh Edition (Oxford University Press, 2016) (excerpt)
2002	Newton's Telecom Dictionary, 30 th Update, Expanded, Anniversary Edition (2016) (excerpt)
2003	The Authoritative Dictionary of IEEE Standards Terms, Seventh Edition (2000) (excerpt)
2004	U.S. Patent Number 11,991,175
2005	Electronic Authentication Guideline (National Institute of Standards and Technology Special Publication 800-63-2, 2013)

I. INTRODUCTION

The Petition challenges claims 14-16 and 18-20 (“Challenged Claims”). All Challenged Claims require exchanging “information related to *authentication*”¹ between an analyte sensor system (*e.g.*, a glucose sensor) and a display device.

An analyte sensor system includes sensitive data about a patient’s health. The ‘222 Patent explains that “where sensitive data is being exchanged, authentication can be used in attempt to prevent *unauthorized* devices or entities from gaining access to the data.” Ex-1001, 58:40-50. The sensor system can authenticate a display device to ensure that the patient’s sensitive health data is not transferred to an “*unauthorized* device[]” (*id.*) and a display device can authenticate a sensor system to ensure “that the data is being received by and from a valid (or approved) device” (*id.*, 61:38-41). Thus, the ‘222 Patent uses “authentication” in accordance with its ordinary meaning which is that authentication involves validating authorization. The ‘222 Patent describes embodiments where an application key that is used to encrypt data during transmission between the sensor system and the display device is also used to perform authentication by validating authorization of the sensor system or the display device.

¹ All emphasis is added throughout unless otherwise indicated.

The Petition has two grounds. Ground 1 alleges obviousness of all Challenged Claims over Yarger (Ex-1005) and Love (Ex-1006). Ground 2 alleges obviousness of all Challenged Claims over Hernandez-Rosas (Ex-1007) and Chivallier (Ex-1008). Petition, 4. Both grounds fail.

Ground 1 relies on Yarger alone to allegedly teach “information related to authentication.” But Yarger does not even perform authentication.

Yarger discloses a glucose sensor that can be paired with a glucose meter to act as a display device to display the sensor’s data. Yarger’s pairing process uses near field communication (NFC) to transfer a secret key from the glucose meter to the sensor. NFC is the type of communication that contactless credit cards use to transfer information to a card reader. Yarger explains that NFC requires that the sensor and glucose meter be brought very close together which minimizes the risk that a third party could intercept the secret key. During the NFC pairing process Yarger’s devices also exchange identifying information that is used to establish a radio frequency (RF) communication link like Bluetooth between them. Yarger’s sensor and glucose meter then communicate via the RF link and encrypt those communications using the secret key to ensure security of the transferred data.

Neither of Yarger’s devices authenticates the other to validate that it is an authorized device to communicate with. Instead, Yarger relies on NFC’s requirement that the devices be in very close proximity and the assumption that a

user will only so closely bring together devices that are authorized to communicate with one another. This is much like a smart credit card does not authenticate a card reader and instead relies on the user to not tap their credit card on a reader the user does not wish to transfer their credit card information to.

Petitioner (“Abbott”) alleges that Yarger’s secret key and identifying information exchanged during NFC pairing corresponds to the claimed “information related to authentication.” But Yarger does not use this information to perform authentication. The Petition’s “Claim Construction” section devotes a single paragraph to purportedly addressing “information related to authentication,” but that section never addresses the meaning of “authentication.” Instead, Abbott points to disclosure in the specification and dependent claims that “information related to authentication” can, *inter alia*, be an application key which can be a random number and alleges that “information related to authentication” must at least encompass a “random number ... related to **identification** of the sensor device or the display device.” Petition, 11-12. There are multiple problems with Abbott’s claim construction analysis.

First, Abbott equates “authentication” with “identification” but these are demonstrably different things. For example, in username/password authentication the username identifies the user and the password authenticates the user.

Second, the fact that the ‘222 Patent describes using an application key that is used to perform encryption to *also perform authentication* in no ways suggests that application keys that are *not* used to perform authentication are somehow “information related to authentication” as claimed.

Ground 1 hinges on Abbott’s improper construction. Abbott alleges that the information exchanged by Yarger during its NFC pairing operation (i.e., a secret key in the form of a random number and identifying information for the sensor and the glucose meter) meets the claimed “information related to authentication.” But Yarger does not use this information to perform authentication by validating authorization of either device. Abbott never even alleges that it does. If the Board gives “authentication” its proper meaning in view of the specification and the ordinary meaning of the term Ground 1 fails.

But Ground 1 also fails for another reason. Abbott fails to establish that Yarger meets even the Petition’s own construction of “information related to authentication.” Yarger’s secret key is only used for encryption. It is in no sense “related to identification of the sensor device or the display device” as required to meet the Petition’s construction. And Yarger’s “identifying information” does not meet the other requirements of the Petition’s construction which alleges that “information related to authentication” encompasses a “random number” or “an exchange of challenge and hash values.” Abbott fails to establish that Yarger’s

devices exchange any information that meets the Petition's construction or is in any way "related to authentication" as required by every Challenged Claim.

Ground 1 fails for that additional reason.

Ground 2 relies on a combination of Hernandez-Rosas and Chivallier.

Ground 2 fails because Abbott fails to establish that a POSA would have combined these references in the manner alleged.

Hernandez-Rosas describes a CGM system in which a glucose sensor authenticates a display device before transmitting analyte sensor data. The display device can advantageously be any of numerous ubiquitous devices like a smart phone, smart watch, a tablet or a desktop or laptop computer. In the Hernandez-Rosas system, authorized display devices must be in possession of secret information known only to authorized devices and the sensor. When a display device seeks to connect with the sensor, the sensor presents the display device with a challenge value and the sensor must perform a hash operation known only to authorized devices using that challenge value and correct sensor identification information and return the correct hash value to the sensor. The sensor only authenticates display devices that return the correct hash value.

Chivallier describes a system in which authentication between a sensor and display device is performed in a different way. Authentication information is stored on a sensor's passive NFC tag. An NFC reader on a display device reads the

sensor's authentication information and the display device compares the sensor's value to a known value for an authorized sensor to authenticate the sensor.

Establishing obviousness requires a supportable reason why a POSA would have combined the references in the manner alleged. Abbott only alleges that a POSA would have been motivated to adopt Chivallier's NFC link for the initial exchange of authentication information in the Hernandez-Rosas system "to prevent the risk of eavesdropping that can occur with other wireless links." This alleged "reason" fails because Hernandez-Rosas does not have a "risk of eavesdropping" vulnerability that Abbott alleges Chivallier's NFC would have prevented.

Hernandez-Rosas's authentication process relies on a secret hash operation only known to the sensor and authorized display devices. This secret hash operation is never transferred between the sensor and display devices so it could not be intercepted by an eavesdropper. Even if an eavesdropper gained access to all the information exchanged during "the initial exchange of authentication information" in Hernandez-Rosas (Petition, 47) that eavesdropper could not pass Hernandez-Rosas's authentication process because the eavesdropper would not have the *secret* hash operation and specific challenge value necessary to do so.

A POSA never would have modified Hernandez-Rosas to use Chivallier's NFC to "prevent the risk of eavesdropping" because Hernandez-Rosas has no vulnerability to eavesdropping. Thus, the *only* reason Abbott alleges for making

Ground 2's combination is entirely unsupported. Ground 2 fails for this reason alone.

Ground 2 also fails for a host of other reasons. The Federal Circuit has made clear that a prerequisite to establishing obviousness is providing a clear explanation of the “contemplated workings” of the combination. Abbott fails to provide that for Ground 2. Abbott's expert says that the Hernandez-Rosas/Chivallier combination adds Chivallier's NFC *tag* and reader to Hernandez-Rosas. Chivallier's NFC tag is a dumb component that only stores a value and transmits it to the reader. It cannot receive or process information. Abbott never explains how Chivallier's NFC tag could be used in Hernandez-Rosas's challenge-response authentication scheme that requires both devices to receive and process information. Abbott's failure to explain the workings of its combination, and its failure to prove that a POSA would have considered Chivallier's NFC tag to be suitable for use in performing Hernandez-Rosas's authentication process, are independent additional reasons why Ground 2 fails.

Finally, Hernandez-Rosas's system advantageously allows the sensor to use as a display various devices that users already have such as a mobile phone, tablet, smart watch, or desktop or laptop computer. These user devices were typically *not NFC-enabled*. If Hernandez-Rosas were modified in the manner Abbott alleges in Ground 2 then authentication would need take place using NFC. That would have

destroyed the ability of Hernandez-Rosas's system to display sensor data on non-NFC-enabled devices of the type Hernandez-Rosas describes. This would have significantly curtailed the flexibility that Hernandez-Rosas emphasizes in being able to use such devices as display devices. Abbott fails to establish that a POSA would have actually made its proposed modification that would have destroyed an important capability of the Hernandez-Rosas system, particularly given that Hernandez-Rosas does not suffer from the eavesdropping risk that is the only reason Abbott alleges would have motivated a POSA to adopt the use of NFC in Hernandez-Rosas in the first place.

Abbott fails to carry its burden for either Ground 1 or Ground 2. Institution should be denied.

II. '222 PATENT

The '222 Patent describes techniques for preserving the battery power of an analyte sensor system configured to wirelessly communicate with multiple different display devices as shown in FIG. 1A (reproduced below). Reducing the frequency at which the battery needs to be replaced "significantly improves the convenience and cost of using [the] analyte sensor system." Ex-1001, 47:40-43.

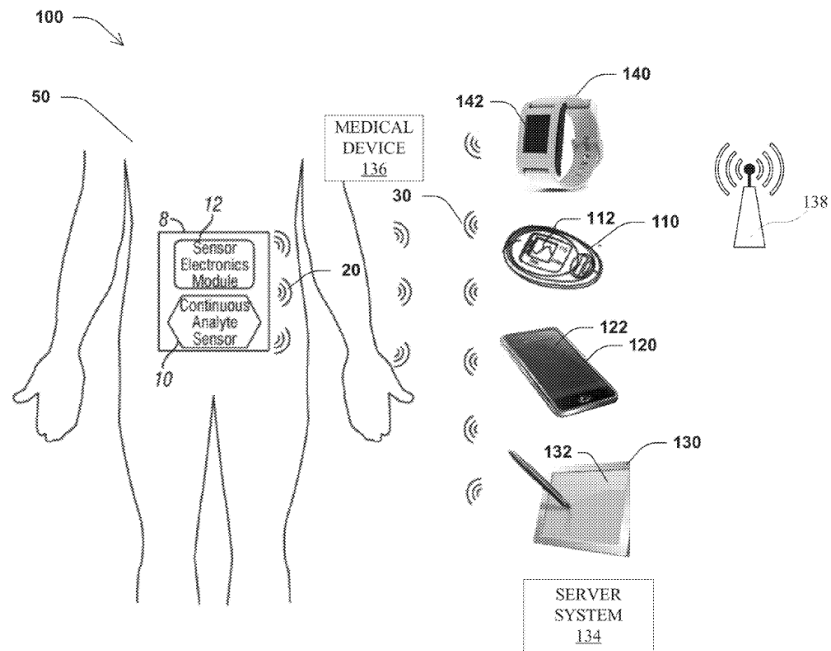


FIG. 1A

Sensor system 308 operates by periodically establishing a wireless connection with one or more display devices to transmit the sensor's measured analyte data via a wireless link, as shown by communication session 720 in FIG. 7A below. Ex-1001, 38:58-62, 46:11-15, 59:17-55, 63:61-64:4. Communication session 720 involves an exchange of numerous messages between the sensor system and display devices that draws power from the sensor system's battery to operate the sensor's wireless transceiver. *Id.*, 64:5-15.

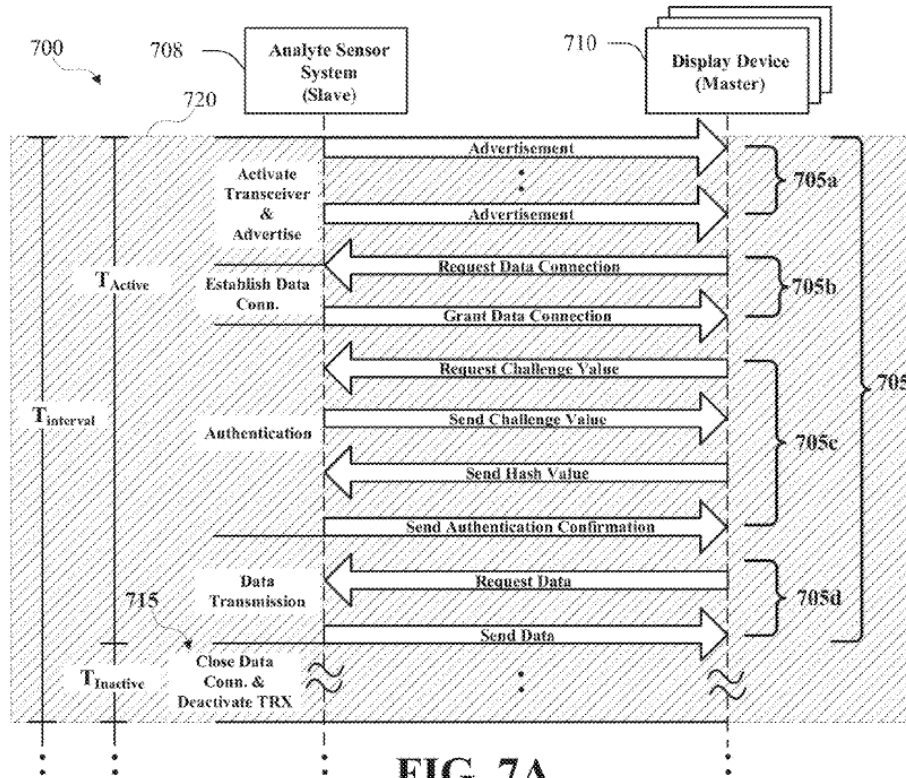


FIG. 7A

For example, to initiate communication session 720, sensor system 708 broadcasts a series of advertisement messages 705a inviting one or more display device to establish a data connection. Ex-1001, 59:56-61, 60:18-36. During operation 705b, a display device receiving an advertisement responds by transmitting a data connection request to sensor system 8 that the sensor system grants or denies. *Id.*, 60:37-40. If a data connection request is granted, sensor system 8 transmits an acknowledgement message to the requesting display 710 and a connection may then be established. *Id.*, 60:40-44.

Before exchanging the sensor's analyte data, authentication operation 705c is performed to verify that one or both of display device 710 and analyte sensor

system 708 are authorized. Ex-1001, 60:44-51. Authentication operation 705c illustrates a one-way authentication in which information related to authentication is exchanged in a challenge and response procedure during which sensor system 8 verifies that display device 710 is authorized to access the sensor's analyte data. *Id.*, 60:52-61:19.

During authentication operation 705c, display device 710 requests a challenge value and sensor system 708 generates and sends a challenge value to display device 710 in response to that request. Ex-1001, 60:52-55. Display device 710 then “generate[s] a hash value based on both the challenge value received from analyte sensor system 708 and identification information associated with analyte sensor system 708” and “transmit[s] the hash value to analyte sensor system 708.” *Id.*, 60:56-61.

Analyte sensor system 708 “receives the hash value from display device 710, decodes the identification information from the hash value, and verifies that the received identification information matches identification information associated with the analyte sensor system 708” stored on the sensor system 708 to validate the hash value. Ex-1001, 60:65-61:5. Alternatively, sensor system 8 can validate the hash value by generating a “mirror hash value” using the same information and comparing the hash value received from the display device to the

mirror hash value generated by the sensor system 8 to verify that they match. *Id.*, 61:5-9.

By validating the hash value received from the display device—either by verifying that the hash value decodes to identification information stored on the sensor system or that the received hash value matches the sensor system’s mirror hash value—sensor system 8 verifies that the display device was in possession of the correct hash function and the correct information to calculate the hash value, and knows the correct information to use in calculating the hash value, thus validating that the display device is authorized to receive the sensor’s data. Ex-1001, 60:6-13, 60:52-61:9, 38:30-48. Sensor system 708 transmits an authentication confirmation to display device 710 if authentication was successful. *Id.*, 61:9-12.

Two-way authentication may also be performed in which additional information is exchanged during authentication operation 705c. Ex-1001, 61:18-22. For example, the above-discussed challenge and response exchange can be repeated in the reverse direction wherein display device 710 generates and transmits a challenge value to sensor system 708 and sensor system 708 responds with a hash value that display device 710 verifies is correct. *Id.*, 61:22-38.

The information related to authentication used to perform challenge and response authentication can include an application key. Ex-1001, 61:50-62:5,

65:47-66:33, 38:30-48. For example, the hash value may be computed based on an application key and the challenge value. *Id.* The application key thus used to authenticate the display device may then also be used to encrypt analyte data exchanged between the sensor and the display after successful authentication. *Id.*, 61:50-62:22. Additionally, an application key may be exchanged as the challenge value during the authentication process and, given that it will be known to both devices after the authentication process, can be used as an encryption key to encrypt data exchange between the sensor and the display after successful authentication. *Id.* The application key used for authentication can in some cases be a randomly generated number and can also be obtained from a server. *Id.*, 61:50-62:53.

After authentication is successful, data can be exchanged “with the understanding that the data is being received by and from a valid (or approved) device.” Ex-1001, 61:38-41. In data transmission operation 705d, display device 710 requests, and sensor system 708 transmits, analyte data to the display device. Ex-1001, 63:40-47.

When sensor system 708 wants to again transmit analyte data to a display device in a subsequent communication interval, communication session 720 is repeated as illustrated in FIG. 7B below. FIG. 7B shows “multiple of occurrences of communication session 720” each performed during a different time interval

T_{interval} with a communication session 720 performed during a first interval, followed by communication session 720' performed during a second interval, etc. Ex-1001, 63:61-64:4.

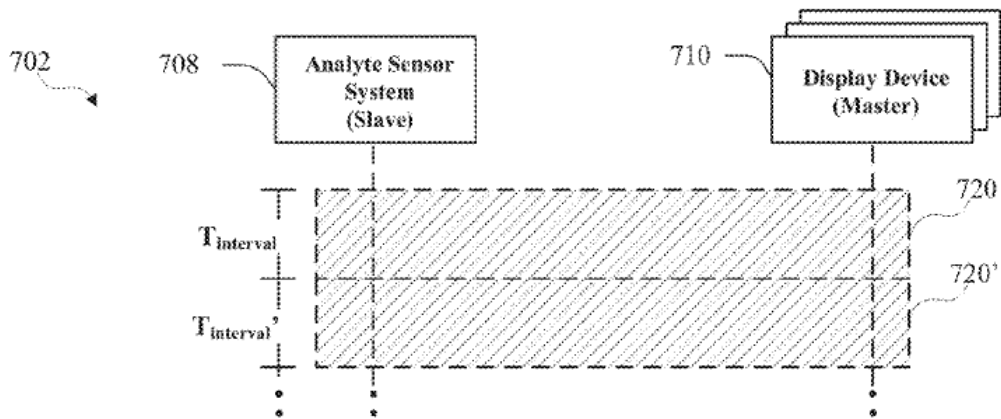


FIG. 7B

To conserve the sensor's battery, the '222 Patent describes performing authentication when a sensor system 8 establishes a connection with a display device for the first time, and bypassing authentication for subsequent communication intervals with the display device to “reduce[] the amount of messaging exchanged between analyte sensor system 708 and display device 710” and thus reduce the power consumption of the sensor. *Id.*, 64:16-35, 65:9-14. FIG. 7C below illustrates an example of this authentication scheme.

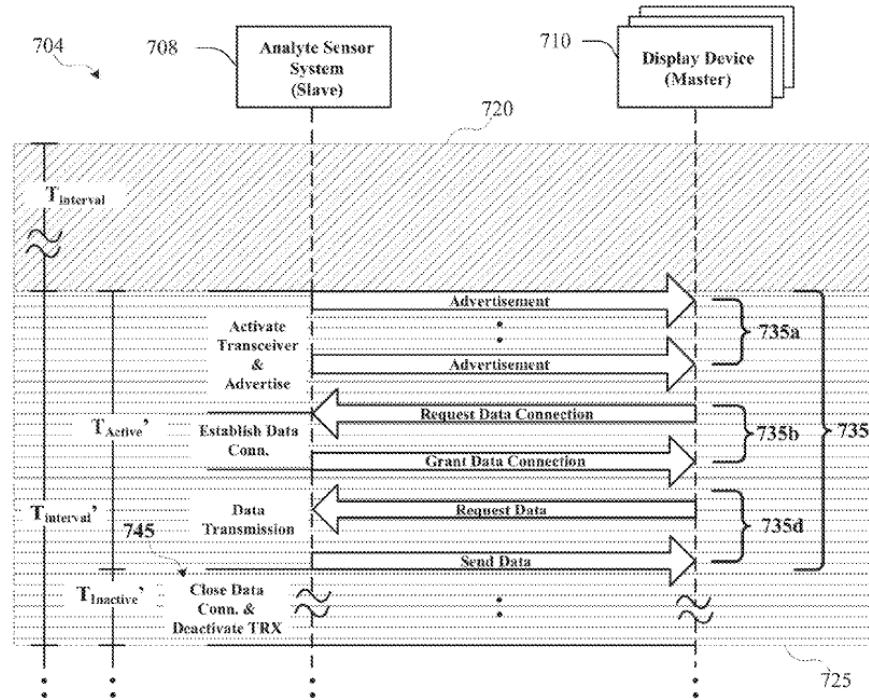


FIG. 7C

During a first time-interval ($T_{interval}$), communication session 720 is performed in the manner discussed in connection with FIG. 7A so that authentication operation 705c is performed to establish the first connection between sensor system 8 and display device 710. Ex-1001, 64:36-47. In a second interval ($T_{interval}'$), a second connection between sensor system 8 and display device 710 is established without performing an authentication operation, as shown by communication session 725. *Id.*, 64:48-66.

By bypassing authentication, the “number of messages exchanged in establishing the second connection (and hence the power consumption) may be reduced.” Ex-1001, 65:9-14. As shown in FIG. 7D below, authentication can be bypassed when establishing a connection during each successive communication

interval, thus significantly reducing the number of messages consuming the sensor system's battery power over the course of communicating with the display device.

Id., 66:58-67:12.

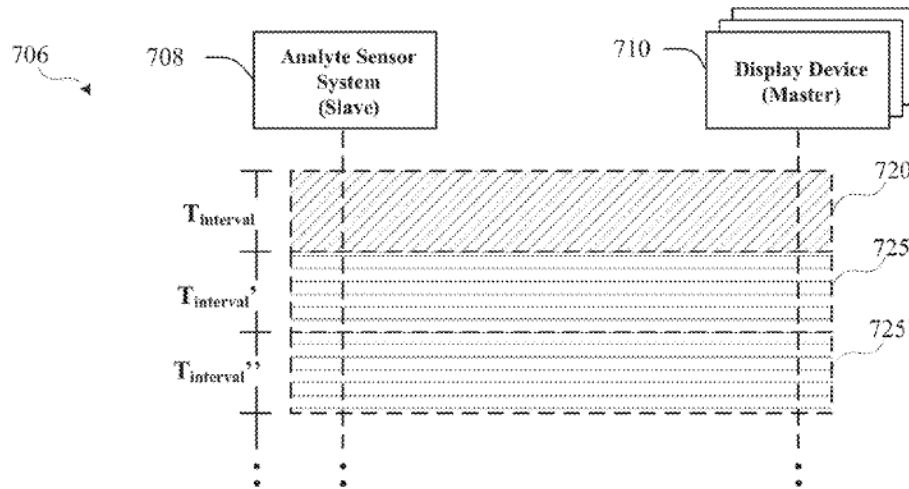


FIG. 7D

III. GROUND 1 FAILS

Ground 1 alleges that the Challenged Claims would have been obvious over Yarger and Love. Petition, 18. Abbott alleges that a POSA would have modified the “CGM system of Yarger” to “adopt the notifications and alarms of the reader device (i.e., display device)” described in Love. Petition, 20. For the limited purpose of this patent owner preliminary response (POPR), DexCom does not challenge that a POSA had reason to adopt Love’s notifications and alarms in Yarger’s CGM system. But Ground 1 fails for other reasons.

Ground 1 fails because the Petition fails to establish that its Yarger-Love combination performs an exchange of “information related to *authentication*” as

required by every Challenged Claim. As detailed below, authentication involves validating authorized access. Yarger does not teach authentication at all. Yarger describes a pairing process between two devices without either one authenticating the other.

A. All Challenged Claims Require an Exchange of “Information Related to Authentication”

All the Challenged Claims require an exchange of “*information related to authentication*.” See Limitations 14[b] and 18[e]. The “information related to authentication” is “exchange[d] ... with a display device” in Limitation 14[b] and is “exchange[d] ... between the analyte sensor system and the display device” in Limitation 18[e].

B. “Authentication” Validates That a Device Is Authorized

The ‘222 Patent uses the term “authentication” consistent with its ordinary meaning, which is validating authorization. In the context of the ‘222 Patent, authentication of a device (a sensor, a display device or both) means validating that the device is authorized to participate in the types of communications described in the ‘222 Patent.

1. The Plain and Ordinary Meaning of “Authentication”

The plain and ordinary meaning in the art of “authentication” is validating that a user or device is authorized to take a specific action. For example, Newton’s Telecom Dictionary (EX2002) defines “authenticate” to mean: “[t]o establish,

usually by challenge and response, that a transmission attempt is **authorized and valid**. To verify the identity of a user, device or other entity in a computer system[.]” Ex-2002, 175. The Authoritative Dictionary of IEEE Standards Terms defines “authentication” as “(1) The process of **validating** a user or process to **verify** that the user or process is **not a counterfeit**. (2) The service used to establish the identity of one station as a member of the set of stations **authorized** to associate with another station.” Ex-2003, 63. The Dictionary of Computer Science (Ex-2001) defines “authentication” as a process by which subjects “establish their identity to a system. This may be effected by the use of a password or possession of a physical device, *e.g.*, a coded token.” Ex-2001, 32.

Other petition-cited evidence confirms that the ordinary meaning of authentication is verifying authorization to take a certain action. For example, Chivallier (Ex-1008)—which is used in Ground 2 and discussed further *infra* §IV.B—describes an authentication process that utilizes private/public key pairs (dual asymmetric key pairs capable of recognizing the other key in the pair). Ex-1008, [0020], [0023], [0029]. In Chivallier, the private key of a private/public key pair is stored in the memory of a passive NFC tag 208 of a sensor module 202 during manufacture to provide “a unique identification of the sensor module 202.” *Id.*, [0020]. The corresponding public key “capable of recognizing a required private key in order to effect an authentication between sensor and mobile device”

(*id.*, [0023]) is stored in the NFC reader of a mobile device 300. Ex-1008, [0017], [0020], [0022]-[0023], [0029].

When the devices are brought into close proximity, the mobile device's NFC reader reads the private key from the sensor module's NFC tag by which the "sensor module 202 identifies itself to the mobile device." Ex-1008, [0028]. In an "**authentication** step" used "to check that the identity of the sensor module 202 is **not a fake** or redundant," the mobile device's public key is "used to recognize and authenticate the private key of sensor 202." Ex-1008, [0029]. *See also*, Ex-1006, [0012] ("authentication...can allow for the detection of **unauthorized** devices); [0108]-[0113] (authenticating a sensor control device using a trusted computer system to verify that an identifier transmitted from the sensor control device to a reader device matches an identifier in a registration database that "associates [a] received identifier 304 with a sensor control device 102 that is **authentic** (e.g., not made by a different manufacturer), or **authorized** for use by the user with reader device 120."); Ex-1007, [0148]-[0150] (describing challenge and response authentication).

2. The Specification Uses the Term “Authentication” Consistent With Its Ordinary Meaning

The specification uses the term “authentication” in its conventional and ordinary way to mean validating authorization.

a. “Authentication” Validates Authorization

The '222 Patent specification has a Section F entitled “Authentication.” Ex-1001, 58:40-71:25. The Authentication section explains that “[i]n scenarios involving the connection of two devices ... authentication may be used ... to prevent *unauthorized* devices from making a connection.” *Id.*, 58:42-45. “[W]here sensitive data is being exchanged, authentication can be used in attempt to prevent *unauthorized* devices or entities from gaining access to the data.” Ex-1001, 58:45-48.

A sensor authenticating a display device to ensure that it is *authorized* to receive sensor data before any patient data is transferred to the display device protects the patient’s privacy by ensuring that their sensitive health data is not transferred to an “*unauthorized* device[.]” Ex-1001, 58:40-50.

A display device authenticating a device to ensure that it is a sensor authorized to transmit data for display on the display device ensures that “data can be exchanged with the understanding that the data is being received by and from *a valid (or approved) device*.” Ex-1001, 61:38-41.

b. Illustrative Embodiments of Authentication

As discussed in the summary of the '222 Patent (§II *supra*), the specification describes performing authentication using a challenge and response exchange in which a display device calculates and transmits a hash value to the sensor system and the sensor system “*validate[s]* the hash value” by either “*verif[ying]*” that the hash value decodes to matching information stored on the sensor system, or by verifying that the hash value received from the display device matches a “mirror hash value” generated by the sensor system. Ex-1001, 60:44-61:9.

An additional challenge and response sequence can be performed with reversed roles so that the display device can verify that the sensor system is authorized to provide sensor data to the display device. Ex-1001, 61:18-38. Once the sensor is authenticated by the display device by validating the hash value received from the sensor, “data can be exchanged with the understanding that the data is being received by and from a valid (or approved) device.” *Id.*, 61:38-41.

Thus, the '222 Patent describes authenticating the sensor, the display device or both to validate that the authenticated device is authorized to communicate with the other. The '222 Patent describes exchanging different types of information between the two devices to authenticate one or both devices. The information used to perform authentication is referred to in the specification as “information related to authentication.” Ex-1001, 2:61-3:30, 3:55-61, 5:24-30, 65:39-66:33.

C. Yarger (Ex-1005) Does Not Teach Authentication

Ground 1 relies entirely on Yarger to purportedly meet Limitations 14[b] and 18[e] their requirement of performing an exchange of “information related to authentication.” Petition, 22-25. Love is not cited to teach this requirement of Limitations 14[b] and 18[e].

1. Overview of Yarger

As discussed in more detail below, Yarger describes a technique to securely transmit data between a glucose sensor and a glucose meter by using encryption. Yarger “pairs” a sensor and glucose meter but neither device authenticates the other. Yarger pairs the sensor and the meter using near field communication (NFC) to establish a connection between them and relies on the user to only bring together devices that are authorized to communicate with one another. Yarger, [0019], [0051].

NFC is the type of inductive coupling communication used by contactless (“tap”) credit card readers. Ex-2004, 4:10-19. NFC requires that devices be brought in *very* close proximity.² “Pairing” the sensor and meter to allow them to communicate requires that the user bring them into the very close proximity required by NFC (Yarger, [0019], [0051]) and issue a user instruction to pair the

² Yarger says 10 cm (less than 4 inches) and Abbott’s expert says “a few centimeters.” Ex-1005, [0018]; Ex-1003, ¶¶34.

devices (Yarger, [0033]-[0034], [0046], FIG. 4 step 410). The “close proximity” required for NFC allows “confidence” in the “security” of this aspect of the pairing process. *Id.*, [0018]-[0019]. “By using an inductive coupling link to perform certain steps of the pairing operation ... the security of the transaction is greatly increased because of the unlikelihood of the short-range, relatively nonstandard inductive coupling transmission being correctly received and decoded.” *Id.*, [0051]. During the NFC pairing process Yarger transfers a secret encryption key (*e.g.*, from the meter to the sensor) that the devices thereafter use to securely communicate over an RF link such as Bluetooth to transfer data. Yarger, [0018], [0022], [0036].

Neither Yarger’s sensor nor its meter “authenticates” the other. Instead, Yarger relies on the fact that NFC requires that the devices be in very close proximity and the assumption that a user will only bring together in such close proximity devices that are authorized to communicate with one another. This is much like a consumer’s credit card. Credit cards do not “authenticate” that a card reader is used by the desired merchant. Instead, credit cards rely on the fact that NFC requires that the credit card be positioned very close to a reader and the assumption that the cardholder will not place their credit card so close to any reader that the user does not wish to transfer their credit card information to. Yarger uses this same principle.

2. Detailed Explanation of Yarger

Yarger relates to a continuous glucose monitoring (CGM) system. CGM systems typically included a glucose sensor attached to the user's skin and a handheld "meter" device that displays glucose measurements from the sensor. Yarger, [0002]-[0003].

In Yarger's CGM shown in FIG. 1, the glucose sensor 110 and the meter 105 communicate wirelessly. Yarger, [0016]. Yarger recognizes that "security" is important and uses a "near field communication (NFC) link" ([0018]) to "securely exchange a secret key that is used to encrypt information on a different wireless link" that the devices use to transfer sensor data from the sensor to the meter ([0016]). *See also* Yarger, [0016], [0018]-[0019], [0022]-[0023], [0050]-[0051]. Yarger's FIGS. 2 and 3 (reproduced below) illustrate glucose meter 105 and glucose sensor 110, respectively. Each includes an NFC transceiver (206 or 306) for exchanging the secret key once the devices are brought close enough together (*e.g.*, 10 cm) to inductively coupled the NFC transceivers' respective inductive elements 208, 308. Yarger, [0018], [0023].

Glucose meter 105 and glucose sensor 110 also include respective RF transceivers 304, 204 to provide a different wireless channel (*e.g.*, Bluetooth®, Bluetooth® low power (BLE), Zigbee®, 802.11) over which sensor data is transmitted between the sensor and the meter. Yarger, [0031].

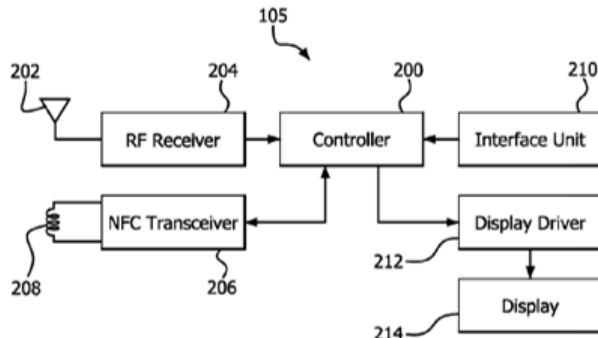


FIG. 2

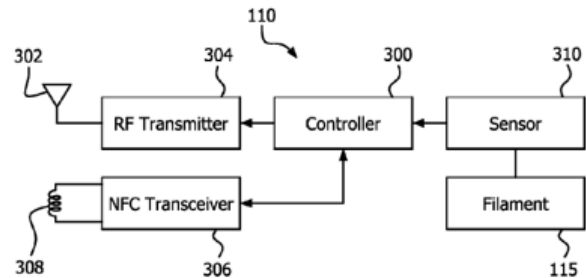


FIG. 3

Yarger FIG. 4 (below left) illustrates a process of securely establishing the wireless RF channel. This process includes exchanging the secret key via the NFC link and using the secret key to encrypt data exchanged over the wireless RF channel. Yarger, [0032]-[0036]. Yarger FIG. 8 (below right) illustrates an example sequence of communications between glucose meter 105 and glucose sensor 110 implementing FIG. 4's process. Yarger, [0032], [0039], [0046].

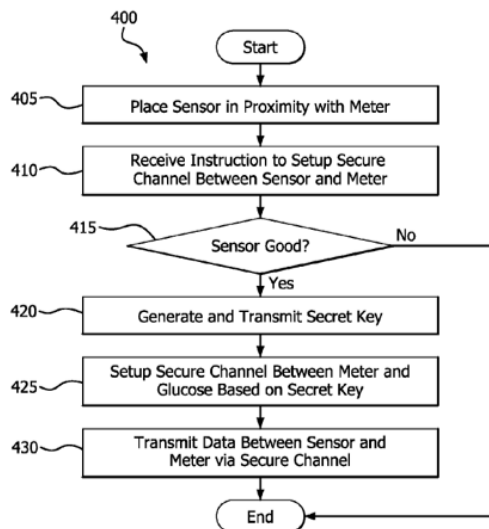


FIG. 4

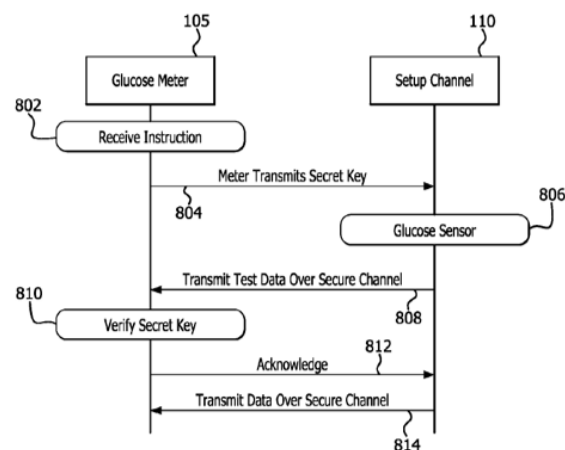


FIG. 8

To begin process 400, "glucose sensor is placed in proximity with the glucose meter" to "initiate an NFC link." Yarger, [0033]. This requires bringing

the devices close enough together (*e.g.*, 10 cm) to inductively couple them. Yarger, [0018]. An instruction is received (*e.g.*, the user may press a button on the glucose meter) to setup a secure channel between the glucose meter and the sensor (steps 410, 802). Yarger, [0033]-[0034], [0046]. An optional check of the sensor's health (*e.g.*, battery power, expiration date, spoilage information, etc.) may be performed (step 415, omitted in FIG. 8). Yarger, [0033]-[0034], [0038].

In response to receiving the instruction to establish a secure channel between the sensor and the meter, “process 400 generates a secret key and transmits the secret key over the NFC link so that both the glucose sensor and the glucose meter share the same secret key ... at step 420.” Yarger, [0035]. In the FIG. 8 sequence, the “glucose meter 105 generates and transmits a secret key at step 804” and “glucose sensor 110 stores the secret key at step 806 to initiate setup [sic] the secure wireless link.”³ Yarger, [0046].

While not shown in FIG. 4 or FIG. 8, Yarger says that during the NFC pairing operation the devices can exchange “identifying information” in addition to exchanging the secret key. Yarger, [0051]. Yarger does not explain what that

³ The “Setup Channel” and “Glucose Sensor” labels for reference numerals 110 and 806 are erroneously switched in FIG. 8 as demonstrated by the text in [0046] and the other sequences in FIGs 5-7.

identifying information is, but a POSA would have understood that it is information from each device that identifies itself to the other as is conventional for a “pairing operation” which is what Yarger describes in [0050]-[0051]. *See e.g.*, Ex-1009, 10 (describing Bluetooth devices exchange unique Bluetooth Device Addresses during pairing).

After the secret key has been exchanged, “the glucose meter and sensor setup a secure wireless channel that is different from the NFC link (e.g., Bluetooth® low power, Zigbee®, a custom wireless link, etc.)” over which data encrypted with the secret key is exchanged. Yarger, [0036], [0046]. The RF wireless channel is “secure” (*id.*) because data transmitted over it is encrypted using the secret key. Yarger, [0046] (“the glucose meter and glucose sensor transmit data over the wireless channel that is encrypted using any suitable encryption algorithm ... using the secret key, thereby forming a secure wireless link.”).

“[T]he CGM system 100 may verify that the secret key was successfully received before transmission of glucose measurement data over the secure wireless link.” Yarger, [0036]. An example of this is shown in steps 808, 810 and 812 of FIG. 8 in which glucose sensor 110 encrypts test data with the secret key and transmits the test data to glucose meter 105 over the secure channel (step 808). Yarger, [0046]. Glucose meter 105 decrypts the test data with the secret key (step

810) and, if the test data is successfully decrypted, “determines that the secret key was successfully received” and transmits an acknowledgement to glucose sensor 110 (step 812). Yarger, [0047]. If the test data was not successfully decrypted, the process returns to step 804 where glucose meter 105 re-transmits the secret key and the sequence of steps is repeated “until the secret key is successfully determined to be received by the glucose sensor 110.” Yarger, [0047].

Thus, Yarger never describes the sensor and meter as “exchang[ing] ... information related to authentication” as required by every Challenged Claim. Instead, Yarger relies on the fact that NFC requires that two NFC-enabled devices be brought into very close proximity to pair, and the assumption that a user of the sensor will not bring it into such close proximity with an unauthorized NFC-enabled meter and instruct the unauthorized meter to pair with the sensor.

D. The Petition Fails to Establish That the Alleged Yarger-Love Combination Exchanges “Information Related to Authentication”

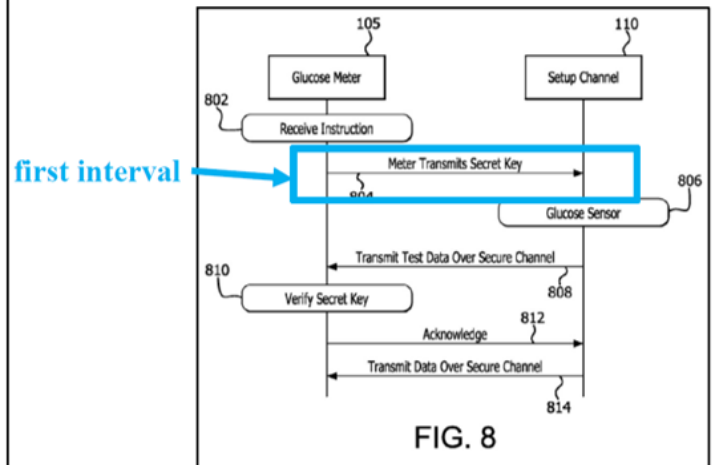
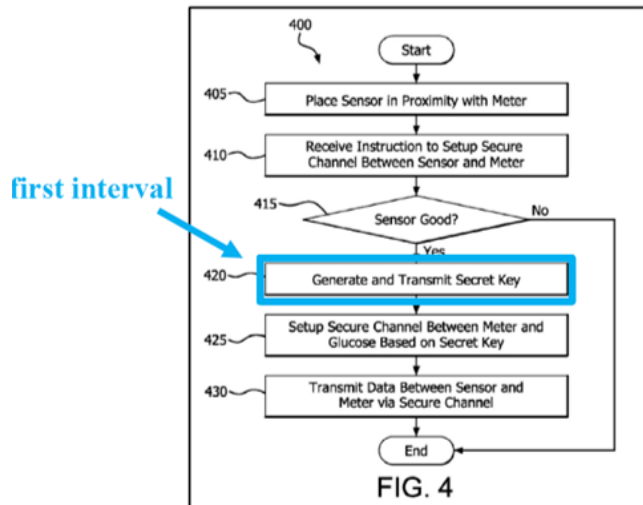
Claim 14 requires “*during a first interval, using a first wireless protocol to perform an exchange of information related to authentication with a display device.*” See Limitation 14[b]. Claim 18 requires “*during a first interval, establish a first connection between the analyte sensor system and a display device*” (Limitation 18[d]) and “*during the first connection, exchange information related to authentication between the analyte sensor system and the display device.*” Limitation 18[e].

The Petition relies entirely on its showing for Limitation 14[b] to meet Limitations 18[d] and 18[e]. *See* Petition, 42 (citing to limitation 14[b] for limitations 18[d] and 18[e]). Thus, DexCom focuses below on the Petition’s showing for Limitation 14[b] because that showing fails and those failings are inherited by Ground 1’s showing for *every* Challenged Claim.

1. Abbott Alleges That Yarger’s NFC Pairing Exchanges “Information Relating to Authentication”

Abbott relies solely on Yarger to meet Limitation 14[b] and does not cite any teachings in Love to meet this limitation. Petition, 22-25.

Abbott alleges that Yarger discloses exchanging “information related to authentication” *during* Yarger’s above-discussed *NFC pairing* operation. Petition, 22 (“Yarger discloses using a first wireless protocol (i.e., near field communication or NFC) to perform pairing, including an exchange of information related to authentication with a CGM’s glucose meter (i.e., a display device), during a first interval.”). Petition, 22. More specifically, Abbott points to step 420 in Yarger’s FIG. 4 (“Generate and Transmit Secret Key”) and step 804 in Yarger’s FIG. 8 (“Meter Transmits Secret Key”) as allegedly meeting the claimed “first interval” during which “information related to authentication” is exchanged. *See* Petition, 23-24 (annotating Yarger’s FIGs. 4 and 8 as reproduced below).



Abbott alleges that Yarger’s “exchange of the ‘*secret key*’ and ‘*identifying information*’ [during the NFC pairing] corresponds to the claimed ‘information related to authentication.’” Petition, 25. As detailed below, Yarger does not disclose using the secret key or identifying information to perform authentication. Abbott fails to establish that this information, either individually or collectively, is “information related to *authentication*” as claimed.

2. Abbott Fails to Give Meaning to the Term “Authentication”

It is black letter law that “meaning should be given to all of a claim’s terms.” *Dell Inc. v. Accelaron, LLC*, 818 F.3d 1293, 1300 (Fed. Cir. 2016); *see also Bicon, Inc. v. Straumann Co.*, 441 F.3d 945, 950 (Fed. Cir. 2006) (“[C]laims are interpreted with an eye toward giving effect to all terms in the claim.”). Despite that, the Petition never meaningfully addresses the meaning of “authentication” or what it requires.

As explained in more detail below, the Petition has a “Claim Construction” section that purports to address the claim term “information related to authentication.” Petition, 11-12. This section never addresses what “authentication” requires. *Id.* Instead, Abbott notes that the specification explains that an “application key” (which can be a random number) or “challenge and hash values” can be used to perform authentication. *Id.* From this, Abbott concludes that “‘information *related to authentication*’ ... at least encompass[es] (i) a random number and (ii) an exchange of challenge and hash values, *related to identification* of the sensor device or the display device.” *Id.*

Thus, Abbott’s claim construction section ends with a sentence that appears to equate “authentication” with “identification.” *No evidence* is cited to support that assertion. Petition, 12. The Petition “must” identify “[h]ow the challenged claim is to be construed” and “[h]ow the construed claim is unpatentable.” 37 C.F.R. §42.104(b)(3)-(4). The en banc Federal Circuit explained that “the specification ‘is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term.’” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1315 (Fed. Cir. 2005). Despite this, Abbott cites nothing in the specification, or even any extrinsic evidence, to support its suggestion that information “related to *identification* of the sensor device or the

display device” is “information related to *authentication*.” Petition, 12 (citing nothing).

It is well understood that identification and authentication are different things. Identification information for a device (or user) is information that uniquely identifies the device (or user), whereas authentication information is information used to validate that the device (or user) is an authorized device (or user). Ex-1008, [0028]-[0029]; *supra* §III.B (“authentication” means validating that a device is authorized as described in the ‘222 Patent specification and consistent with the ordinary meaning). For example, in the ubiquitous username and password authentication technique, the username is identification information that uniquely identifies the user and the password is authentication information that is used to validate that the person seeking to login is an authorized user.

Abbott’s showing is facially deficient. Abbott never even alleges, let alone establishes, that Yarger performs an authentication process that validates that the sensor device or the display device is an authorized device. As detailed below, Abbott wholly fails to establish that Yarger discloses that either its secret key or its identification information exchanged during pairing is “information related to *authentication*.”

3. Abbott Fails to Establish That Yarger’s “Secret Key” Is “Information Related to Authentication”

a. Yarger’s Secret Key Is Not Used for Authentication

As discussed *supra* §III.C, Yarger’s secret key is “randomly generated data” exchanged via the NFC link “for encrypting communications between the glucose meter 105 and the glucose sensor 110” to secure communications over a separate RF link such as Bluetooth. Yarger, [0018]; *see also* Yarger, [0035]-[0036], [0046], [0051]. In the FIG. 8 communication sequence (reproduced below), the “glucose meter 105 generates and transmits a secret key ... at step 804” and “glucose sensor 110 stores the secret key at step 806.” Yarger, [0046].

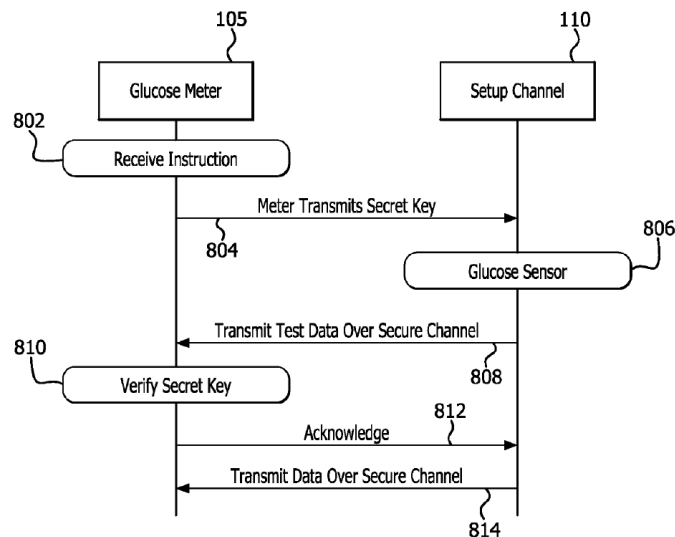


FIG. 8

An RF wireless channel distinct from the NFC link is setup and made secure by encrypting the data exchanged over the wireless channel using the secret key that was exchanged over the NFC link. Yarger, [0036] (“the glucose meter and glucose sensor transmit data over the wireless channel that is *encrypted* using any

suitable encryption algorithm ... using the secret key, thereby forming a secure wireless link.”). In the FIG. 8 sequence, glucose sensor 110 encrypts test data using the secret key and transmits it over the secure wireless channel (step 808) and glucose meter 105 decrypts the received test data to verify “that the secret key was successfully received by the glucose sensor 110” (step 810). Yarger, [0047].

Yarger never says that the secret key is used to perform authentication. Instead, Yarger teaches only that the secret key is used to encrypt communications over Yarger’s RF link.

b. Abbott Fails to Establish That Yarger’s Secret Key Is “Information Related to Authentication”

The Petition has a single paragraph that purports to establish that Yarger’s “secret key” (and “identifying information”) meets the claimed “information related to authentication.” Petition, 25. As explained *supra* §III.D.2, this paragraph ignores the meaning of “authentication” and makes arguments that are entirely unsupported.

i. Abbott’s argument fails as a matter of claim construction

Abbott alleges that “[t]he claimed ‘information related to authentication’ at least encompasses a random number related to identification of the sensor device or the display device, *as explained above in Section VI.A*” and “Yarger’s secret key can be a random number” that is exchanged along with “identifying information”

during Yarger’s pairing operation so Yarger’s secret key meets the claimed “information related to authentication.” *Id.*

DexCom does not dispute that Yarger’s secret key can be a random number. But Abbott’s argument fails as a matter of claim construction because Abbott’s assertion that “[t]he claimed ‘information related to **authentication**’ at least encompasses a random number related to **identification** of the sensor device or the display device” is false. *Id.* Abbott ignores that Yarger’s “secret key” is not **used for authentication** the way that keys disclosed in the ’222 Patent specification are. Abbott’s suggestion that **any** “random number related to identification of the sensor device or the display device” is “information related to authentication”—even if it is not used to perform authentication—fails as a matter of claim construction because it reads “authentication” out of the claims.

Abbott relies entirely on the Petition’s “Section VI.A” to purportedly establish that “‘information related to authentication’ at least encompasses a random number related to identification of the sensor device or the display device.” *Id.* “Section VI.A” is the Petition’s “Claim Construction” section. Petition, 11-12.

Abbott’s Claim Construction Section (§VI) discusses two claim terms — “information related to authentication” and “application key.” Petition, 11-12. Abbott identifies a random number as an example of information used by

embodiments in the ‘222 Patent specification to perform authentication.⁴ *Id.*

Abbott then erroneously suggests that *any* “**random number** ... related to **identification** of the sensor device or the display device” must meet the claimed “information related to authentication” irrespective of whether that random number is used to perform authentication. *Id.* Abbott’s claim construction fails because it gives no meaning to “information related to **authentication**.” *See supra* §III.B. (“authentication” means validating that a device is authorized as described in the ‘222 Patent specification and consistent with the ordinary meaning) and *supra* §III.D.2 (identification and authentication of a device are different things).

More specifically, Abbott alleges that dependent claim 16 “make[s] clear that the ‘information related to authentication’ can comprise an ‘application key’” because claim 16 says “the information related to authentication comprises an application key.” Petition, 11. Abbott then cites portions of the ’222 Patent specification stating that an “application key” can comprise a “random number” and can include “a challenge and hash value.” *Id.* From this, Abbott alleges that “the claim terms ‘information related to authentication’ and ‘application key’ both

⁴ Abbott also identifies an exchange of challenge and hash values as information used in the specification to perform authentication. Petition, 11-12.

at least encompass (i) a random number and (ii) an exchange of challenge and hash values, related to identification of the sensor or the display.” Petition, 12.

Abbott’s logic is flawed. The fact that the specification describes an embodiment where a key (which can be random number) is used to perform authentication does not mean that *every* random number key—including a key that is *not* in used to perform authentication—is somehow “information related to authentication.”

As discussed in Section II above that provides an overview of the ‘222 Patent specification, in one embodiment a key (which can be a random number) is used to perform authentication in a challenge and response authentication process in which the key is used to calculate hash values during an authentication process that determines whether the sensor or display device is an authorized device. Ex-1001, 61:50-62:5, 38:33-40. Thus, a key in the ‘222 Patent is “information related to authentication” when that key is used in an authentication process to validate that a device is authorized.

Yarger does not use its secret key in the manner the ‘222 Patent describes to validate that a device is authorized. Abbott never even alleges that it does. Yarger uses the secret key exchanged between the sensor and display devices over Yarger’s NFC connection only to encrypt subsequent RF communications between the sensor and the display. Yarger, [0018], [0022], [0036]; *supra* §III.C

(summarizing Yarger). Indeed, Yarger is explicit about the purpose of “exchang[ing] cryptographic keys and identifying information.” Yarger, [0051]. The purpose is not to perform authentication by validating that either of the devices is authorized to communicate but instead to “ensure[] that *subsequent communication* between the device 110 and 105 *is secure*” because those subsequent communications are encrypted using the secret key. Yarger, [0051].

As detailed above, Abbott’s claim construction that alleges that an application key (which can be a random number) meets “information related to *authentication*” if it is “related to *identification* of the sensor device or the display device” fails because authentication and identification are different things. *See supra* §III.D.2; *see also supra* §III.B (“authentication” means validating that a device is authorized as described in the ‘222 Patent specification and consistent with the ordinary meaning). If the Board agrees, Abbott’s reliance on Yarger’s secret key to allegedly meet the claimed “information related to authentication” in Limitations 14[b] and 18[e] must be rejected because Abbott’s argument hinges entirely on its improper claim construction.

Abbott never even alleges, let alone establishes, that Yarger’s secret key is used to validate that any device is authorized and thus fails to establish that Yarger’s secret key is “information related to *authentication*” under the proper construction of “authentication.”

ii. Abbott fails to establish that Yarger’s secret key meets Abbott’s own construction of “information related to authentication” because Yarger’s key is not “related to identification” of any device

Even if the Board were to find that Abbott’s claim construction were correct that “‘information related to *authentication*’ at least encompasses a random number related to *identification* of the sensor device or the display device” (it is not), Abbott’s reliance on Yarger’s secret key still fails because Abbott fails to establish that Yarger’s secret key meets Abbott’s own construction. Petition, 11-12, 25. Specifically, Abbott fails to establish that Yarger’s random number secret key is “related to identification of the sensor device or the display device” as required to meet Abbott’s construction. *Id.*, 12. Thus, the Petition fails to have “Content” that it “must” have because the Petition fails to identify “[h]ow the construed claim is unpatentable.” 37 C.F.R. §42.104(b)(4).

Abbott alleges that “‘information related to *authentication*’ at least encompasses a random number related to *identification* of the sensor device or the display device” and alleges that Yarger’s secret key “can be a random number.” Petition, 25. But the Petition never even alleges that Yarger’s secret key—as opposed to separate “identifying information” in Yarger—is “related to identification of the sensor device or the display device” as required to meet Abbott’s construction, let alone explain how or why that would allegedly be so. *Id.*

To the extent the Petition is read to suggest that Yarger’s secret key identifies the sensor or display device, nothing in Yarger supports that. As discussed *supra* §III.D.3.a, Yarger uses the secret key for one purpose—to encrypt data over the RF communication channel. Abbott never explains how or why a key only used for encryption is somehow “related to identification.” Petition, 25. Indeed, Abbott relies on a key in Yarger that is a “**random** number.” *Id.* A random number is not a unique identifier of any device and Abbott never explains how a **random** number could somehow be “related to identification” of any device.

Abbott’s argument is an exercise in obfuscation. In its claim construction section, Abbott alleges that “information related to authentication” is met by “a random number ... related to identification of the sensor device or the display device.” Petition, 12. But in mapping Yarger to Limitation 14[b], Abbott never alleges that Yarger’s random number key is “related to identification of the sensor device or the display device.” Petition, 25. Instead, Abbott points to different “identifying information” in Yarger that “permits the display device to identify the sensor device.” *Id.* Abbott’s claim construction section never alleged that **any** and all information “related to identification of the sensor device or the display device” could meet the claimed “information related to authentication.” Petition, 12. Abbott only alleged that a “random number” or “an exchange of challenged and hash values” that “related to identification of the sensor device or the display

device” would meet the claimed “information related to authentication.” Petition, 12. In mapping Yarger to Limitation 14[b], Abbott fails to identify any information that meets its construction because it is “a random number” or “an exchange of challenge and hash values” that *also* is “related to identification of the sensor device or the display device.” *Id.*

More specifically, in purporting to map Yarger to Limitation 14[b], Abbott alleges that during Yarger’s NFC “initial ‘pairing’ operation” there is “an exchange of this secret key *and ‘identifying information’*” and that “the exchange of the secret *key and ‘identifying information’*⁵ permits the display device to identify the sensor device.” Petition, 25. Abbott never even alleges, let alone establishes, that Yarger’s secret key—as opposed to the “identifying information” exchanged during the pairing operation—is in any way “related to identification of the sensor device or the display device.” *Id.*

Thus, Abbott fails to establish that Yarger’s secret key meets even Abbott’s own construction of “information related to authentication.”

⁵ Yarger’s “identifying information” is not used for authentication as discussed *infra* § III.D.4 immediately below.

iii. Abbott’s separate assertion that determining whether the secret key was exchanged is “authentication” fails

In connection with a different claim limitation (Limitation 18[f]) that requires determining “whether authentication was performed during the first interval,” Abbott alleges that Yarger meets this and performs authentication by determining “whether the secret key was successfully exchanged.” Petition, 42 (citing *nothing*). That argument inexplicably equates verifying the exchange of the secret key with “authentication.” This argument fails for three reasons.

First, not a single piece of evidence is cited to support that verifying successful exchange of the secret key is authentication. Petition, 42. Abbott cannot carry its burden with naked attorney argument.

Second, Abbott’s unsupported assertion is facially false. Verifying that the secret key was successfully received does not authenticate anything. When Yarger’s display device determines that the secret key was not successfully received by a sensor, Yarger does not determine that the sensor is an unauthorized sensor. Instead, Yarger’s display device simply retransmits the key to the sensor and continues to do so “until the secret key is successfully determined to be received by the glucose sensor 110.” Yarger, [0047]; *supra* §III.C.2. Thus, the determination by Yarger’s display device of “whether the secret key was successfully exchanged” (Petition, 42) does not perform authentication because it

does not validate whether the sensor is an authorized sensor. *Supra* §III.B (“authentication” means validating that a device is authorized as described in the ‘222 Patent specification and consistent with the ordinary meaning).

c. Conclusion—Abbott Fails to Establish That Yarger’s Secret Key is “Information Related to Authentication”

As demonstrated above, Abbott not does establish that Yarger’s secret is used for any purpose other than to encrypt communications, let alone establish that it is used—like keys in the ‘222 Patent—to perform authentication by validating that either Yarger’s sensor or display device is an authorized device.

Abbott fails to establish that Yarger’s secret key is in any respect “information related to authentication,” and indeed fails to establish that Yarger’s secret key meets even Abbott’s own construction for this claim term.

4. Abbott Fails to Establish That Yarger’s “Identifying Information” Is “Information Related to Authentication”

In purporting to map Limitation 14[b] to Yarger, Abbott alleges that “the exchange of the ‘secret key’ and ‘*identifying information*’ corresponds to the claimed ‘information related to authentication.’” Petition, 25.

Abbott’s reliance on Yarger’s “identifying information” fails because it does not meet Abbott’s own construction of “information related to authentication” and because “identifying information” is not “information related to authentication.”

a. Yarger’s “Identifying Information” Does Not Meet Abbott’s Own Construction of “Information Related to Authentication”

Abbott’s claim construction alleges that “‘information related to authentication’ ... at least encompass[es] (i) *random number* and (ii) *an exchange of challenge and hash values*, related to identification of the sensor device or the display device.” Petition, 12. Abbott does not even allege, let alone establish, that Yarger’s “identifying information” is a random number or an exchange of challenge and hash values. Petition, 25.

Thus, Abbott’s reliance on Yarger’s “identifying information” fails because it does not meet Abbott’s own construction of “information related to authentication.” 37 C.F.R. §42.104(b)(4) (the Petition “must” identify “[h]ow the *construed* claim is unpatentable”).

b. Abbott Fails to Establish That Yarger’s “Identifying Information” Is “Information Related to Authentication”

Abbott points to Yarger’s disclosure that the NFC “pairing operation” allows the devices to “exchange cryptographic key and *identifying information* that ensures that subsequent communication between the device 110 and 105 is secure.” Yarger, [0051]. This single use of “identifying information” in Yarger, [0051] is the only time that Yarger uses the term “identifying information.”

i. Identifying information is not authentication information

Yarger does not explain what the “identifying information” is that is exchanged during the NFC “pairing operation” because this was well known. Yarger, [0051]. Pairing is a mutual registering of identification information between two devices that allows the devices to thereafter communicate and is akin to two people exchanging phone numbers so they can thereafter communicate. *See e.g.*, Ex-1009, 10 (Bluetooth devices exchange unique Bluetooth Device Address during pairing).

Pairing by exchanging identifying information is not authentication because neither device validates the other device or determines whether the other device is authorized to do anything. *See supra* §III.B (“authentication” means validating that a device is authorized as described in the ‘222 Patent specification and consistent with the ordinary meaning).

ii. Yarger does not perform “authenticated pairing”

Abbott obfuscates by suggesting that Yarger’s use of NFC for pairing and setting up a Bluetooth link was understood in the art to be authentication. Petition, 13 (fn. 2). This assertion, which Abbott relegates to a footnote, does not withstand even slight scrutiny. In its footnote argument, Abbott cites Ex-1009 which the Petition’s quotation reveals refers to something called “**authenticated pairing**.”

Petition, 13 (quoting Ex-1009, 7). Ex-1009 states that “NFC can simplify the process of *authenticated pairing* between two Bluetooth devices by exchanging authentication information over an NFC link.” Ex-1009, 7. Ex-1009’s reference to using NFC for authenticated pairing is irrelevant to Ground 1 because Yarger does not disclose *authenticated* pairing.

Initially, to the extent that Abbott suggests that Ex-1009 describes all Bluetooth pairing as performing authentication that is false. Ex-1009 does not say that Bluetooth pairing authenticates, and Bluetooth pairing in fact does not perform authentication. As the Board is undoubtedly aware from its own use of Bluetooth-enabled devices, the Bluetooth standard allows *any* two Bluetooth-enabled devices to pair and establish a Bluetooth connection—not just certain authorized devices. Pairing two devices involves exchanging identifying information between them. This is what enables a user of a Bluetooth-enabled phone to know what device(s) the phone is paired to because the devices identify themselves to each other during pairing. But no authentication is performed by one device of the other to validate that the device is authorized to do anything. *See Supra* §III.B (“authentication” means validating that a device is authorized as described in the ‘222 Patent specification and consistent with the ordinary meaning).

The “authenticated pairing” referenced in Ex-1009 is different than the simple pairing that Yarger describes. While Ex-1009 does not provide details about

what “authenticated pairing” is, this was known in the art. As an example, Abbott’s own Chivallier (Ex-1008) reference describes an example of authenticated pairing and uses NFC to exchange authentication information precisely as stated by Ex-1009.

In Chivallier’s authenticated pairing process, a mobile device’s NFC reader reads a private key from a sensor. Ex-1008, [0029]. The private key provides “a unique identification of the sensor module 202.” *Id.*, [0020]. But the mobile device does not simply take the sensor’s identification of itself at face value and immediately pair with the sensor to allow subsequent communication. Instead, the mobile device performs an “*authentication step* in order to check that the identity of the sensor module 202 is *not a fake or redundant*.” *Id.*, [0029]. The mobile device authenticates the sensor by using a corresponding public key held by the mobile device “to recognize and *authenticate* the private key of sensor 202.” *Id.* Only if there is a “match[] between the [sensor’s] private stored key... and the [mobile device’s] public stored key ... is [the sensor] *fully authenticated* as being the sensor module 202 compatible with the mobile device 300. Thereafter any communication between the sensor 202 and mobile device 300, in accordance with the private and public keys, will be encrypted so all data will only be readable by the sensor 202 and device 300.” *Id.*

Thus, in Chivallier’s *authenticated* pairing process, the sensor’s private key is used for *two* purposes: (1) it is used by the mobile device to authenticate the sensor as a sensor authorized to communicate with the mobile device and (2) it is “[t]hereafter” used to encrypt communications between the sensor and the mobile device. Ex-1008, [0029]. Yarger only describes its secret key that is exchanged during Yarger’s NFC pairing process as being used for the second of these two purposes—to encrypt subsequent communications over the RF link. Yarger, [0018], [0022], [0036]. Yarger does not describe using its secret key to authenticate one of the devices to validate that it is authorized to communicate with the other.

After describing authentication, Chivallier describes a “pairing step” which involves exchanging identifying information between the devices and using this identifying information to establish a connection between the devices. Ex-1008, [0030]. Chivallier says that “the pairing process could be part of the authentication process.” *Id.* But simply pairing the devices by exchanging identifying information, without performing the authentication process Chivallier describes to validate and “*authenticate[]*” the sensor as “compatible with the mobile device,” is not authentication and Chivallier never says that it is. Ex-1008, [0029]-[0030].

As detailed above, Abbott’s assertion that the identification information that Yarger’s devices exchange during NFC pairing is “information related to

authentication” is unsupported by anything in the ‘222 Patent, Yarger or any other reference. Yarger performs simple pairing—not “authenticated pairing.”

5. Abbott Fails to Establish That Yarger’s “Secret Key” and “Identifying Information” Together Are “Information Related to Authentication”

To the extent that Abbott relies on Yarger’s “secret key” and “identifying information” to somehow collectively be “information related to authentication” that assertion fails. Petition, 25. As demonstrated *supra* §§III.D.3-III.D.4, neither Yarger’s secret key nor its identifying information has anything to do with authentication. Abbott cannot fabricate “information related to authentication” from two different pieces of information in Yarger that have nothing to do with authentication.

Neither Yarger’s sensor nor its display device authenticates the other. Yarger relies entirely on the “security” that NFC provides—“because of the unlikelihood of the short-range, relatively nonstandard inductive coupling transmission being correctly received and decoded”—to ensure that a user will only pair two authorized devices. Yarger, [0051]; *supra* §III.C.

Abbott fails to establish that Yarger’s devices exchange any “information related to authentication.”

6. Abbott's Expert Testimony Cannot Save Ground 1

The only other evidence that Abbott cites to support its assertion that Yarger teaches exchanging “information related to authentication” is a single paragraph of expert testimony. Petition, 25 (citing Ex-1003, ¶82). This testimony parrots *verbatim* the Petition's argument. *Compare* Ex-1003, ¶82 *with* Petition, 25 (the second, third and fourth sentences of the first full paragraph). Indeed, the declaration even inherits a broken reference link from the Petition at 25. This testimony cannot save Ground 1 for two reasons.

First, this testimony warrants no weight under the Board's precedential *Xerox* decision because it repeats the Petition's arguments word-for-word without providing any meaningful analysis or corroborating evidence. *Xerox v. Bytemark*, IPR2022-00624, Paper 9, 15 (Aug. 24, 2022) (precedential) (“[T]he 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.”) (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”)).

Second, the cited expert testimony adds nothing to Abbott's argument. It repeats the same arguments as in the Petition in the same words. The expert's testimony—just like the Petition's arguments—is unsupported by Yarger or any

other evidence supporting the assertion that the information Yarger exchanges during its NFC pairing is “information related to authentication” as claimed.

E. Conclusion—Ground 1 fails

As detailed above, the Petition fails to establish that its alleged Yarger-Love combination meets exchanging “information related to authentication” as required by both challenged independent claims. *See* Limitations 14[b] and 18[e]. Thus, Ground 1 fails.

IV. GROUND 2 FAILS

A. Hernandez-Rosas (Ex-1007)

Hernandez-Rosas discloses a CGM system in which a sensor system is configured to communicate with various types of display devices (*e.g.*, a custom analyte monitoring device 110, a mobile phone 120, a tablet 130, a smart watch 140) to wirelessly transmit analyte sensor data to the display device for display. Hernandez-Rosas, [0122], [0124], [0127]; FIG. 1 (below).

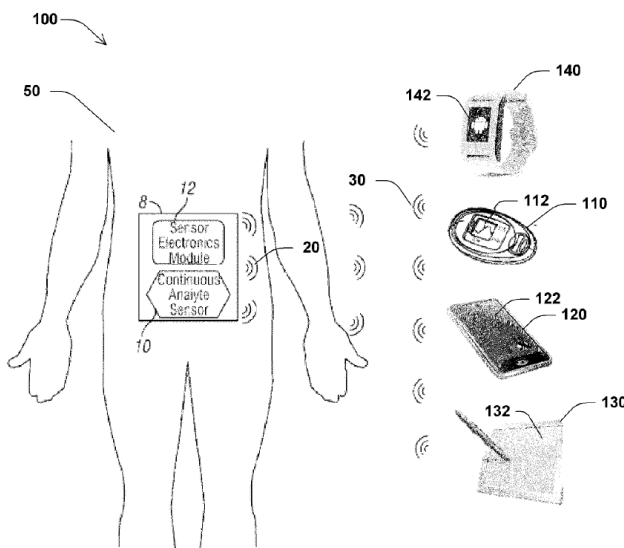


FIG. 1

Sensor system 8 is configured to support being in direct wireless communication with *multiple* display devices simultaneously. Hernandez-Rosas, [0109], [0128], [0140]-[0141].

As illustrated in FIG. 3 reproduced below, analyte sensor system 8 includes a transceiver 316 for wirelessly transmitting analyte data measured by analyte sensor 312 (corresponding to sensor 10 in FIG. 1 above) to a transceiver 338 of one or more of the display devices. *Id.*, [0139], [0142]. Examples of suitable wireless protocols to exchange data between sensor system 8 and a display device include “WiFi, Bluetooth and Bluetooth Low Energy (BLE).” *Id.*, [0141].

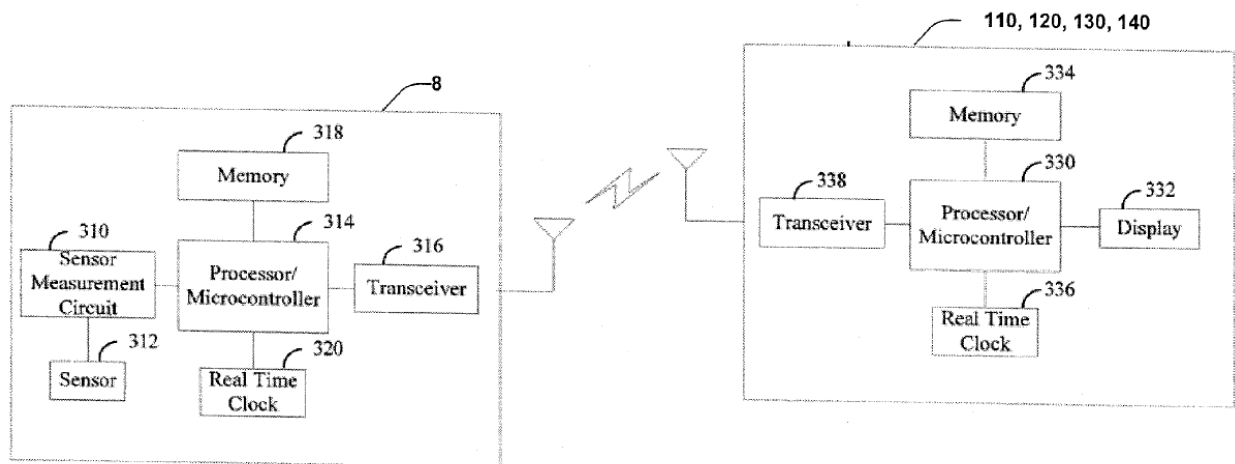


FIG. 3

To conserve battery power, sensor system 8 alternates between inactive periods in which sensor system 8 is in “sleep mode” and active periods in which the sensor wakes up and establishes a wireless connection with one or more display

devices 110, 120, 130, 140 to transmit analyte data to the display. Hernandez-Rosas, [0147].

Upon waking up, sensor system 8 activates its transceiver 316 to broadcast a series of “advertisement signals,” each of which is “an invitation for a display device 110, 120, 130, 140 to establish a data connection.” *Id.*, [0148]. Sensor system 8 establishes a data connection with one or more display devices that respond to the advertisement signal(s), transmits analyte data over the established wireless connection and then returns to sleep mode. *Id.*, [0148]-[0151]. If sensor system 8 has not previously established a connection (paired) with a display device that responds to an advertisement signal, an authentication process is performed as part of establishing the wireless data connection. Hernandez-Rosas, [0148]-[0149].

Hernandez-Rosas’s FIG. 4 (reproduced below) illustrates two different communication sessions 410 and 420 between sensor system 8 and a display device where at the end of each session 410 and 420 the sensor system terminates the wireless connection and reenters sleep mode. *Id.*, [0148]-[0151].

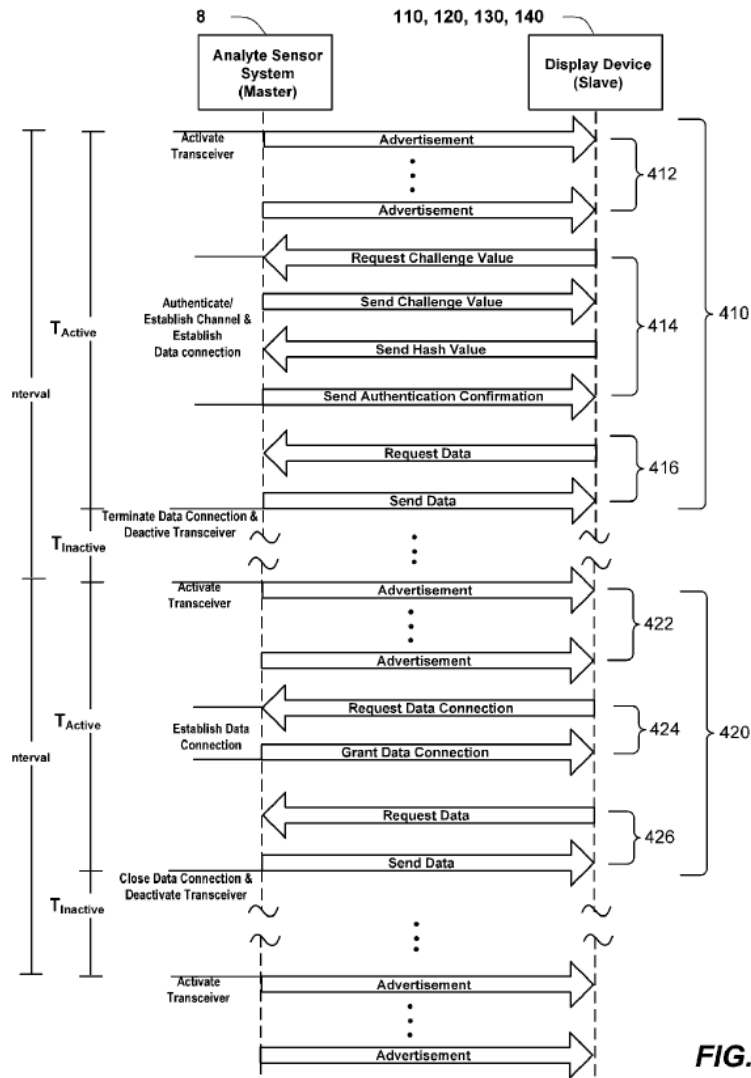


FIG. 4

As shown in FIG. 4, each communication session begins with the sensor system broadcasting “a series of advertisement signals 412,” where each advertisement signal is an “invitation for a display device 110, 120, 130, 140 to establish a data connection.” Hernandez-Rosas, [0148]. Communication session 410 illustrates the communication sequence performed when a display device that sensor system 8 has not previously paired with responds to an advertisement signal so that “an authentication procedure needs to be performed as part of a data

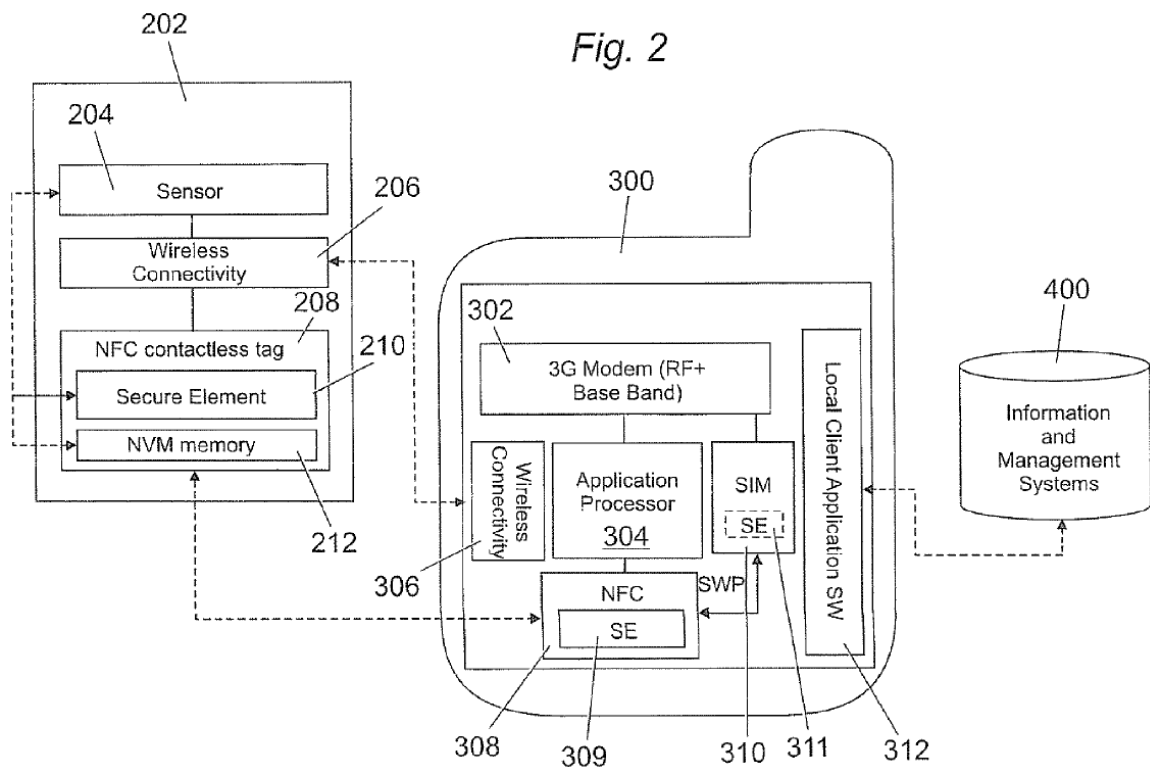
connection process 414.” *Id.*, [0148]-[0149]. As shown by the arrows in process 414, a challenge and response exchange is performed to authenticate the display device in the following manner.

Initially, the display device “requests a challenge value from ... sensor system 8” and the sensor system 8 “sends the change [*sic*, challenge] value to the display device in response.” *Id.*, [0150]. Upon receiving the challenge value, the display device calculates a “hash value” based on the challenge value and the “identification information associated with the analyte sensor system 8” input by the user into a custom application running on the display device and sends the hash value to sensor system 8. *Id.*, [0149]-[0150]. Sensor system 8 receives the hash value from the display device, “decodes the identification information from the hash value, and verifies that the received identification information matches [the] identification information” stored on the sensor system (*e.g.*, during manufacture). *Id.*, [0150].

Upon verification, sensor system 8 sends “a signal confirming a successful authentication” to the display device. *Id.*, [0150]. After completing connection and authentication process 414, sensor system 8 and the display device engage in data communication session 416 during which the display device requests and receives analyte data. *Id.*, [0151].

B. Chivallier (Ex-1008)

Chivallier discloses a technique to provide secure transmission of data between a sensor module 202 and a mobile device 300. Chivallier, Fig. 2 (reproduced below). Chivallier uses an NFC link to perform authentication before activating RF transceivers to establish a wireless RF channel over which sensor data is transmitted between the sensor and mobile device.



Sensor module 202 comprises a passive NFC contactless tag 208 having a secure element 210 that stores a private key in its non-volatile (NVM) memory 212. Chivallier, [0017], [0020]. The private key is loaded during manufacturing of the sensor module 202. *Id.*, [0017], [0020]. Non-volatile memory 212 also stores health parameters measured by sensor 204 (e.g., while the user is wearing the

device). Chivallier, [0019]. Sensor module 202 further includes a wireless connectivity module 206 for communicating with wireless connectivity module 306 of mobile device 300. Chivallier, [0016], [0030].

Mobile device 300 includes an NFC reader 308 for reading the private key stored in NVM 212 of the sensor module's passive NFC tag 208. Chivallier, [0020]-[0022], [0028]. NFC reader 308 includes a secure element 309 that stores "a public key which is capable of recognizing a required private key in order to effect an authentication between sensor and mobile device." Chivallier, [0023]. This authentication is performed prior to establishing a connection between sensor module 204 and mobile device 300 for data transmission via their respective wireless connectivity modules 206, 306. Chivallier, [0028]-[0030].

Before establishing a wireless connection to transmit sensor data, "the user must bring the sensor module 202 and the mobile device 300 into close proximity" (Chivallier, [0028]) so that NFC reader 308 can read the "private key [that] allows [for] a unique identification of the sensor module 202." Chivallier, [0020]. This private key is stored on sensor module 202's NFC tag 208 and uniquely identifies the sensor. *Id.*, [0020]. The public key stored on mobile device 300's NFC reader is "used to recognize and authenticate the private key of the sensor 202" to "check that the identity of the sensor module 202 is not a fake or redundant." Chivallier,

[0029]. If sensor module 202 is authenticated, connection modules 206 and 306 are activated and sensor module 202 and mobile device are paired. Chivallier, [0030].

C. Ground 2 Fails Because the Petition Does Not Establish That a POSA Would Have Combined Hernandez-Rosas in the Way the Petition Alleges

Establishing obviousness requires establishing some non-hindsight reason to modify the prior art references *in the manner claimed*. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007); *TQ Delta, LLC v. CISCO Sys., Inc.*, 942 F.3d 1352, 1359 (Fed. Cir. 2019) (reversing the Board’s obviousness determination; “a conclusory assertion with no explanation is inadequate to support a finding that there would have been a motivation to combine because ‘this type of finding, without more, tracks the *ex post* reasoning *KSR* warned of and *fails to identify any actual reason why a skilled artisan would have combined the elements in the manner claimed.*’”) (internal citation omitted). To demonstrate any Challenged Claim obvious, Abbott needed to establish some reason why a POSA “would have selected and combined [the] prior art elements” in a manner that “*yield[s] the claimed invention.*” *Unigene Labs., Inc. v. Apotex, Inc.*, 655 F.3d 1352, 1360 (Fed. Cir. 2011).

The Petition offers a single reason why a POSA allegedly would have modified Hernandez-Rosas based on Chivallier. Abbott alleges that a POSA would have understood that it was important to ensure that a “wireless link used to

transmit [] authentication and encryption information is secure from eavesdropping” to prevent “an unauthorized device [from] ...mimic[king] the authentication steps.” Petition, 46. Abbott alleges that because the “range of an NFC communication is on the order of a few centimeters” a POSA would have understood that Chivallier’s NFC link is “effective to prevent eavesdroppers” from intercepting Chivallier’s private key. Petition, 47. Based on this, Abbott alleges that a POSA “would have been motivated to adopt Chivallier’s use of the short-range NFC to exchange information related to authentication in the CGM system of Hernandez-Rosas in order to achieve Hernandez’s stated goal of providing for authentication in order *to prevent the risk of eavesdropping* that can occur with other wireless links.” Petition, 47. Abbott alleges that a POSA would “adopt[] the NFC link of Chivallier for the initial exchange of authentication information” in the Hernandez-Rosas CGM system. *Id.*

Abbott’s assertion that a POSA would have adopted Chivallier’s use of NFC “to prevent the risk of eavesdropping” fails for numerous reasons detailed below.

First, Hernandez-Rosas does not have the “risk of eavesdropping” vulnerability that Abbott alleges Chivallier’s use of NFC would prevent. Any eavesdropper that gained access to the information exchanged during “the initial exchange of authentication information” in Hernandez-Rosas (Petition, 47) would not be able to pass Hernandez-Rosas’s authentication process because that process

relies on the devices employing hash information that is only known to authorized devices. A POSA would not have modified Hernandez-Rosas in the manner Abbott alleges to address an “eavesdropping” vulnerability that Hernandez-Rosas simply does not have.

Second, Abbott ignores particular aspects of how Hernandez-Rosas’s challenge-response authentication scheme works that a POSA would have understood made Chivallier’s passive NFC tag and NFC reader approach unsuitable for use in the Hernandez-Rosas system. For example, Hernandez-Rosas employs a multi-step authentication exchange that requires *active* participation of both devices and is not amenable to being performed using Chivallier’s NFC communication that uses a *passive* NFC tag on one device that is simply read by an NFC reader on the other. Furthermore, introducing an NFC link into Hernandez-Rosas’s CGM system would limit the display devices the sensor could work with to *NFC-enabled* devices which would have severely limited the ability of Hernandez-Rosas’s system to work with many of the types of devices that Hernandez-Rosas describes as suitable display devices (mobile phones, tablets, smart watches, desktop or laptop computers). A POSA never would have diminished the usability of the Hernandez-Rosas system in this way, particularly where doing so was entirely unnecessary given that the Hernandez-Rosas system is

immune from the eavesdropping risk that Abbott alleges would have motivated the combination.

Abbott fails to establish that a POSA would have made the alleged combination of Hernandez-Rosas and Chivallier. Ground 2 fails.

1. Hernandez-Rosas is Immune From the Alleged Eavesdropping Risk

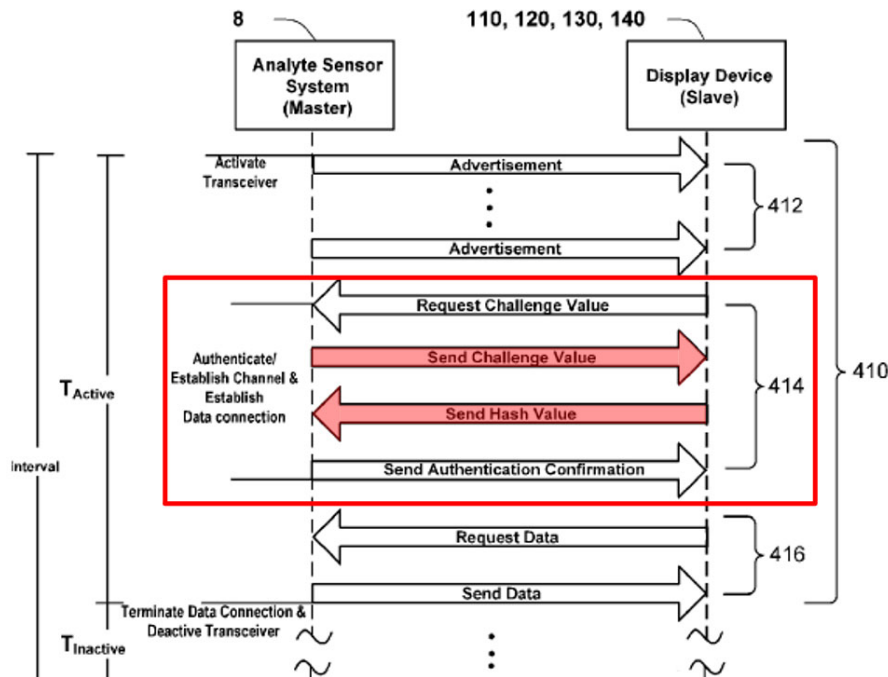
Hernandez-Rosas's devices exchange information related to authentication during the authentication process performed in connection process 414 boxed in **red** in the excerpt of Hernandez-Rosas's FIG. 4 below. *See also* §IV.A *supra*.

Even if an eavesdropper intercepted all of this information, no unauthorized device would have been able to make use of this information to gain access because an eavesdropper would still lack information needed to be successfully authenticated in the Hernandez-Rosas authentication process.

In Hernandez-Rosas's authentication exchange, the display device must receive a challenge value sent from the sensor system for that exchange, calculate a hash value from the challenge value and the identification information associated with the sensor system 8 entered by the user into the custom application running on the display device, as shown in the steps shaded in **red** below. Hernandez-Rosas, [0149]-[0150].

To be authenticated, the display device must possess (1) the challenge value sent by the sensor system, (2) the correct sensor identification information stored

by the sensor, (3) the correct hash function expected by the sensor system, and (4) the knowledge to use both (1) and (2) in calculating a valid hash value. Hernandez-Rosas, [0150]. Failure to possess all of this information would result in an incorrect hash value being sent to the sensor system that would fail the sensor system’s verification of the received hash value. *Id.*



Abbott fails to identify any information exchanged during “the initial exchange of authentication information” in Hernandez-Rosas that would create risk of unauthorized access if intercepted by an eavesdropper. Petition, 47. That is because there is no such information. *Id.* Indeed, Hernandez-Rosas implements a well-known challenge-response protocol that was known to prevent the very replay attacks—i.e., “mimic[king] the authentication steps” (Petition, 46)—that the Petition identified as the alleged vulnerability in Hernandez-Rosas that could be

exploited by eavesdropping. Hernandez-Rosas, [0019], [0150]; Ex-2005, 7, 11, 73 (describing challenge-response protocols and replay attacks).

In Hernandez-Rosas's challenge-response authentication, an eavesdropper would not be able to use an intercepted "exchange of authentication information" in an attempt to pose as an authorized display device in a subsequent authentication attempt because the eavesdropper would still lack the correct hash function and sensor identification information needed to calculate a valid hash value, neither of which are exchanged between the display device and sensor system. Hernandez-Rosas, [0149]-[0150]; Ex-2005, 10, 54 (describing functions). Thus, an eavesdropper would be unable to generate and return the correct hash value that the sensor will require before authenticating a display device. Hernandez-Rosas, [0149]-[0150].

An eavesdropper also would not be able to use an intercepted hash value returned by an authorized display device in an attempt to spoof the identify of that authorized display device because the intercepted hash value was calculated using the specific challenge value received from the sensor system by the authorized display device during its challenge-response exchange. Hernandez-Rosas, [0150]; Ex-2005, 7, 11, 73. Thus, if an imposter device sought to be authenticated by the sensor using the intercepted hash value in a subsequent challenge-response exchange, the sensor would reject that hash value because it would not be the

correct hash value for the different challenge value sent to the imposter device.

Thus, stealing a hash value would not allow an imposter device to be authenticated by the sensor. *Id.*

As demonstrated above, it is an authorized device's possession of the correct way to generate a hash value (i.e., the correct hash function applied to the correct information) that the sensor uses to verify that a display device is authorized, and that information is not exchanged between the sensor and display devices and thus is not at risk of being discovered by an eavesdropper. Hernandez-Rosas, [0149]-[0150]. Interception of information exchanged between devices during Hernandez-Rosas's "initial exchange of authentication information" (Petition, 47) does not create a security risk in Hernandez-Rosas because it would not allow an eavesdropping imposter device to be authenticated by the sensor and gain access.

"Prevent[ing] the risk of eavesdropping" is the ***only reason*** Abbott identifies as to why a POSA allegedly "would have motivated to adopt Chivallier's use of the short-range NFC link ... for the initial exchange of authentication information." Petition, 47. As demonstrated above, that alleged reason is entirely unsupported. That is fatal to Ground 2's obviousness showing. *KSR*, 550 U.S. at 418 (a supportable reason to combine the references in the manner claimed is required to establish obviousness); *TQ Delta*, 942 F.3d at 1359 (same); *Unigene*

Labs., 655 F.3d at 1360 (a reason is required for why a POSA “would have selected and combined [the] prior art elements” in a manner that “yield[s] the claimed invention.”).

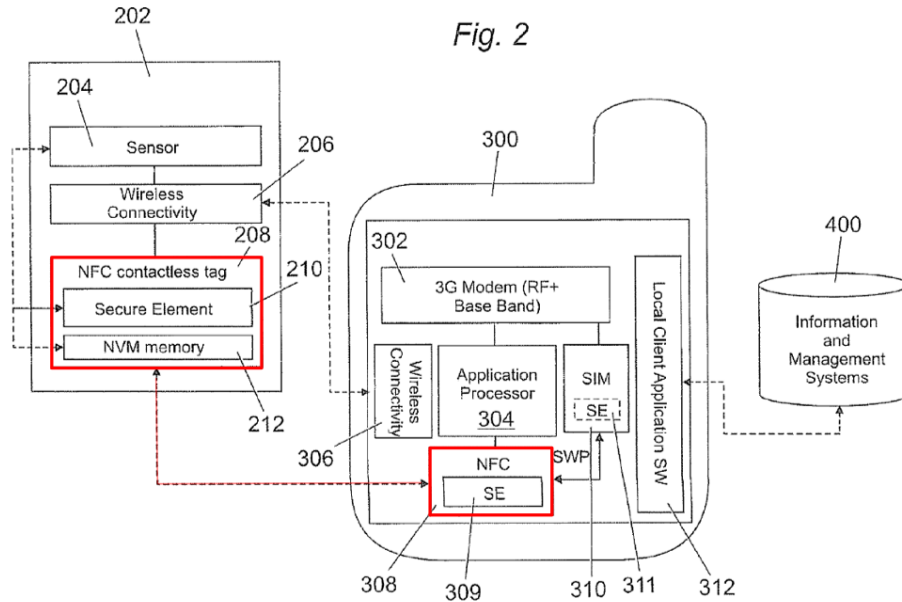
The Board routinely denies institution where an obviousness ground fails to establish a supportable reason to combine the references. *See e.g., Truist Bank v. United Services Automobile Association*, IPR2023-00143, Paper 15 at 25-26 (May 16, 2023) (“[W]e determine that ***Petitioner has failed to show that a skilled artisan would have been motivated to combine the teachings*** of Acharya and King as set forth in sole independent claim 1 of the ’432 patent and as proposed in the Petition. ***On this basis, Petition has failed to show a reasonable likelihood of prevailing*** with respect to any of the claims challenged in the Petition. We, therefore, deny the Petition and do not institute inter partes review.”); *Hewlett Packard Enterprise Co. v. K.Mizra LLC*, IPR2022-00843, Paper 14 at 22 (Oct. 31, 2022) (“***Due to the lack of a sufficient motivation to combine, Petitioner has not shown a reasonable likelihood of proving claim 1 unpatentable*** over the combination of Gleichauf, Ovadia, and Lewis. And, for the same reasons, Petitioner has not shown a reasonable likelihood of proving independent claims 10 and 17 or dependent claims 2–9, 11–16, and 18–20 unpatentable.”).

The Petition’s failure to establish a supportable reason to combine the teachings of Hernandez-Rosas and Chivallier in the manner alleged is fatal to Ground 2. Ground 2 should be denied for this reason alone.

2. The Petition Fails to Explain the Contemplated Workings of the Combination

The Federal Circuit has made clear that “a *prerequisite* to adequately explaining and supporting a conclusion” of obviousness is “a clear, evidence-supported account of the *contemplated workings of the combination*.” *Pers. WebTechs., LLC v. Apple, Inc.*, 848 F.3d 987, 994 (Fed. Cir. 2017).

The Petition proposes adopting “Chivallier’s use of the short-range NFC link to exchange information related to authentication in the CGM system of Hernandez-Rosas.” Petition, 47. As shown in Chivallier’s Fig. 2, Chivallier’s “use of the short-range NFC link” is to provide a *passive* NFC tag on the sensor and an NFC reader on the mobile device to perform the simple task of reading the passive tag to obtain the sensor’s private key stored therein. *See also supra* §IV.B.



Petitioner’s expert explains that the Hernandez-Rosas/Chivallier combination “add[s] the NFC **tag** and reader of Chivallier” to Hernandez-Rosas. Ex-1003, ¶161. But Chivallier’s “NFC tag” simply stores a value and, when powered on by being brought into proximity with the NFC reader, transmits that stored value to the NFC reader. Chivallier, [0017], [0020].

As discussed in Section IV.C.3 immediately below, Chivallier’s passive NFC tag (which does not receive or process information) is entirely unsuitable for use in Hernandez-Rosas’s authentication process which is a multi-step challenge-response process that requires that both devices be capable of receiving and processing information. But DexCom bears no burden in this proceeding. It was Abbott’s burden to explain the contemplated workings of its combination. Yet, neither the Petition nor Abbott’s expert even attempts to explain how Chivallier’s

passive “NFC tag” allegedly would have worked in Hernandez-Rosas’s multi-step authentication process that requires that both devices be capable of receiving and processing information.

Ground 2 fails for this additional reason because Abbott fails to make a “prerequisite” showing required for establishing obviousness by explaining “the contemplated workings of the combination.” *Pers. WebTechs.*, 848 F.3d at 994.

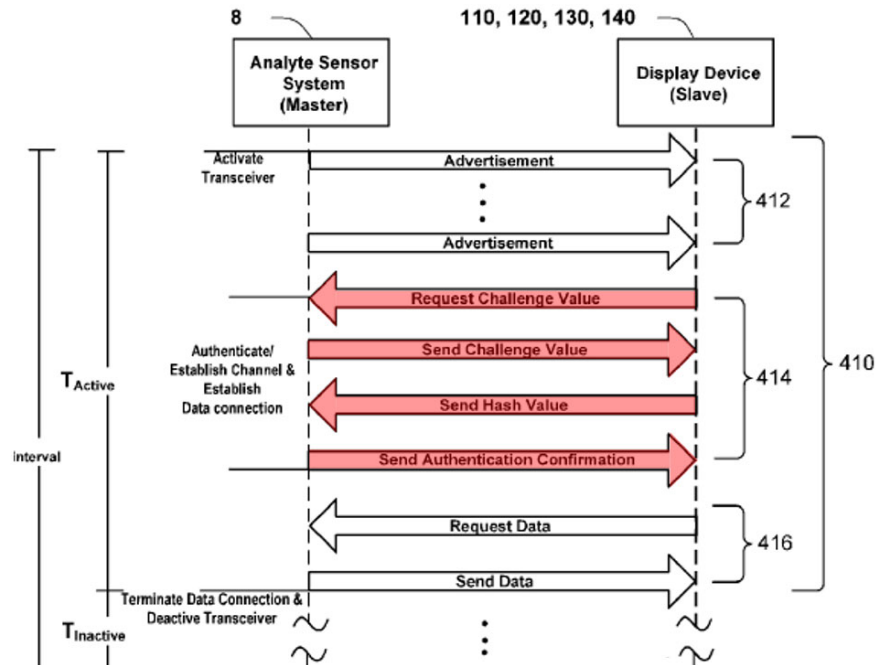
3. Abbott Ignores Reasons Why a POSA Would Not Have Used Chivallier’s Passive NFC Tag and NFC Reader to Exchange Hernandez-Rosas’s Authentication Information

The prior art references must be considered in their entirety including portions that would have led a POSA away from combining the references in the manner claimed. *Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve, Inc.*, 796 F.2d 443, 448-449 (Fed. Cir. 1986) citing *W.L. Gore & Assoc., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1550 (Fed. Cir. 1983). Abbott ignores a host of such reasons.

a. Hernandez-Rosas’s Four-Step Challenge-Response Authentication Process Is Incompatible with NFC That Chivallier Uses for Its Simple One-Step Private Key Sharing

The Petition alleges that a POSA would have used NFC for the “initial exchange of authentication information” in Hernandez-Rosas. Petition, 47. This “initial exchange of authentication information,” shaded in red in Hernandez-Rosas’s FIG. 4 below, is far more complicated than the initial exchange of

authentication information in Chivallier where an NFC reader simply reads a value from a passive NFC tag.



Hernandez-Rosas involves a four step bi-directional challenge-response exchange between the display device and the sensor whereby (1) the *display device* requests a challenge value, (2) the *sensor* generates and transmits to the display device a new challenge value, (3) the *display device* computes a hash value and transmits the hash value to the sensor, and (4) the *sensor* decodes and verifies that the hash value is correct (which indicates that the display device is an authorized display device) and sends the display device an authentication confirmation.

Abbot fails to even acknowledge the dramatic differences between the “initial exchange of authentication information” (Petition, 47) in Hernandez-Rosas as compared to Chivallier. Chivallier’s passive NFC tag and NFC reader that

Abbott's expert alleges a POSA would have added to Hernandez-Rosas (Ex-1003, ¶161) is entirely unsuitable for use in the Hernandez-Rosas authentication process.

A passive NFC tag could not be used to perform the role of the display device in the Hernandez-Rosas authentication process which requires (in step 3 above) that the display device receive a challenge value, calculate a hash value using that challenge value and sensor identification information. Hernandez-Rosas, [0150].

A passive NFC tag also could not be used to perform the role of the sensor in the Hernandez-Rosas authentication process which requires that the sensor be capable of receiving the hash value returned from the display device and processing that received hash value to verify that it is the correct value (step 4 above). Hernandez-Rosas, [0150].

Abbott fails to establish that Chivallier's use of a passive NFC tag and NFC reader to perform a simple one-step exchange of authentication information stored on the tag would have motivated a POSA to use "the NFC link of Chivallier" to perform the four-step authentication process in Hernandez-Rosas that requires that both devices be capable of receiving and processing information. Petition, 47.

**b. Using NFC to Exchange Authentication Information
Would Have Eliminated Numerous Display Devices
That Hernandez-Rosas Teaches Are Desirable**

One of the goals of the Hernandez-Rosas system is to allow the sensor to use a variety of different types of devices as display devices, including ubiquitous devices that users already have for other purposes such as a mobile phone, a tablet, a smart watch, or a desktop or laptop computer. Hernandez-Rosas, [0109], [0122], [0124], [0127]-[0128], Fig. 1.

Typical mobile phones, tablets, smart watches, and desktop and laptop computers were not NFC-enabled devices. If Hernandez-Rosas were modified in the manner alleged by Abbott so that authentication would need take place using NFC, that would have eliminated the ability of the sensor in Hernandez-Rosas to display sensor data on non-NFC-enabled devices like a mobile phone, tablet, smart watch and a desktop or laptop computer. This would have significantly curtailed the flexibility Hernandez-Rosas emphasizes in being able to use such devices as display devices. Hernandez-Rosas, [0109].

Abbott fails to establish that a POSA would have actually made the proposed modification to Hernandez-Rosas that would have significantly impacted the flexibility of the system, particularly given that Hernandez-Rosas does not suffer from the eavesdropping risk that Abbott alleges would have motivated a POSA to adopt the use of NFC in Hernandez-Rosas.

4. Conclusion—Ground 2 Fails

As detailed above, Abbott fails to carry its burden to demonstrate what is required to establish obviousness because it establishes no supportable reason why a POSA would have combined Hernandez-Rosas and Chivallier in the manner alleged and fails to explain the contemplated workings of the combination. That is fatal to Ground 2.

V. CONCLUSION

The Petition fails to demonstrate that it is reasonably likely to show that any Challenged Claim is unpatentable. The Board should deny institution.

Respectfully submitted,
DexCom, Inc.

Date: August 22, 2024

/Richard Giunta/

Richard F. Giunta, Reg. No. 36,149
WOLF, GREENFIELD & SACKS, P.C.

CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. §42.24, the undersigned certifies that the foregoing **PATENT OWNER'S PRELIMINARY RESPONSE** contains 13,743 words excluding; a table of contents, a table of authorities, a certificate of service or word count, or appendix of exhibits or claim listing. Patent Owner has relied on the word count feature of the word processing system used to create this paper in making this certification.

Date: August 22, 2024

/Dara Del Rosario/
Dara Del Rosario
Paralegal
WOLF, GREENFIELD & SACKS, P.C.

CERTIFICATE OF SERVICE UNDER 37 C.F.R. §42.6 (e)(4)

I certify that on August 22, 2024, I will cause a copy of the foregoing document, including any exhibits filed therewith, to be served via electronic mail, as previously consented to by Petitioner, upon the following:

Scott C. Weidenfeller

sweidenfeller@cov.com

Peter P. Chen

pchen@cov.com

David A. Garr

dgarr@cov.com

abbott-ipr@cov.com

Date: August 22, 2024

/Dara Del Rosario/

Dara Del Rosario

Paralegal

WOLF, GREENFIELD & SACKS, P.C.