NOTE: This disposition is nonprecedential.

United States Court of Appeals for the Federal Circuit

VERIFY SMART CORP.,
Appellant

v.

ASKELADDEN, L.L.C.,
Appellee

UNITED STATES,
Intervenor

2019-1076

Appeal from the United States Patent and Trademark Office, Patent Trial and Appeal Board in No. IPR2017-00726.

Decided: August 5, 2020

STEVEN M. HOFFBERG, Tully Rinckey PLLC, New York, NY, for appellant. Also represented by JEAN-MARC ZIMMERMAN, Zimmerman Law Group, Westfield, NJ.

RICHARD L. RAINEY, Covington & Burling LLP, Washington, DC, for appellee. Also represented by DOUGLAS ALEXANDER BEHRENS, BRIAN GERARD BIELUCH; MARK

BERKOWITZ, CHARLES R. MACEDO, Amster Rothstein & Ebenstein LLP, New York, NY.

DENNIS FAN, Appellate Staff, Civil Division, United States Department of Justice, Washington, DC, for intervenor. Also represented by SCOTT R. MCINTOSH, ETHAN P. DAVIS; THOMAS W. KRAUSE, FARHEENA YASMEEN RASHEED, Office of the Solicitor, United States Patent and Trademark Office, Alexandria, VA.

Before LOURIE, SCHALL, and DYK, *Circuit Judges.*

LOURIE, *Circuit Judge.*

Verify Smart Corp. ("Verify") appeals from the final written decision of the United States Patent and Trademark Office Patent Trial and Appeal Board ("the Board") holding claims 1–19 of U.S. Patent 8,825,648 ("the '648 patent") unpatentable as obvious. *See Askeladden LLC v. Verify Smart Corp.*, No. IPR2017-00726, 2018 WL 3572368 (P.T.A.B. July 23, 2018) ("*Decision*"). Because the Board did not err in its conclusion that the challenged claims would have been obvious over the prior art, we affirm.

BACKGROUND

Verify owns the '648 patent, which is directed to systems and methods for verifying a user's identity in electronic transactions. The patent relates to multi-factor authentication, which utilizes secure information that the user knows as well as an electronic communications device (*e.g.*, a phone) in the user's possession. For example, the patent provides that "a user and the user's communication device are pre-enrolled in a verification program" administered by a verifier (*i.e.*, the user's bank) and the verifier operates a database that stores a secure identifier for the user (*e.g.*, a password or personal identification number ("PIN")) as well as an identifier for the user's electronic device (*e.g.*, an access number). *See, e.g.*, '648 patent col. 4 ll. 5–8, 27–

29. When the user attempts to make a transaction, the verifier attempts to open a communications link with the user's device, and once the communications link is open, the verifier sends an identification verification request ("IVR") to the device, which displays the request to the user. *Id*. col. 4 ll. 38–46. The user then responds to the IVR by inputting the correct secure identifier and sending the response back to the verifier through the open communications link. *Id*. col. 4 ll. 48–51. The verifier then compares the secure identifier entered by the user with the secure identifier stored in the database and permits the transaction to proceed if there is a match. *Id*. col. 4 ll. 54–61.

Claim 1 is illustrative and recites:

> 1. A user identity verification method for verifying the identity of a user by a verifier in the course of an electronic transaction, said user identity verification method comprising the steps of:
>
> (a) pre-enrolling the user, comprising the steps of:
>
> (a1) assigning to the user a bona fide secure identifier; and,
>
> (a2) storing the bona fide secure identifier in a database that is accessible to the verifier;
>
> (b) pre-enrolling a user communications device, wherein pre-enrolling the user communications device comprises the steps of:
>
> (b1) obtaining a user access number for the user communications device, wherein the user access number can be used to open a communications link with the user communications device; and,
>
> (b2) storing the user access number in a database that is accessible to the verifier;

> (c) retrieving the user access number stored at Step (b2);
>
> (d) opening a communications link between the verifier and the user communications device by using the user access number retrieved at Step (c);
>
> (e) sending an identity verification request (IVR) from the verifier to the user through the communications link opened at Step (d);
>
> (f) inputting by the user a putative secure identifier;
>
> (g) sending through the communications link opened at Step (d) a response to the IVR of Step (e);
>
> (h) retrieving the bona fide secure identifier stored at Step (a2);
>
> (i) comparing the putative secure identifier input at Step (f) with the bona fide secure identifier retrieved at Step (h); and,
>
> (j) allowing the transaction to proceed only if the comparison of Step (i) results in a match between the putative secure identifier and the bona fide secure identifier.

'648 patent col. 18 l. 63–col. 19 l. 31.

Askeladden, LLC ("Askeladden") is a single-member limited liability company formed by The Clearing House Payments Company, LLC ("TCH"), which in turn is owned by twenty-five of the world's largest commercial banks, including Bank of America (collectively the "member banks"). Askeladden filed a petition for *inter partes* review of claims 1–19 of the '648 patent, arguing that the claims were unpatentable as obvious over a combination of U.S. Patent App. Pub. 2005/0184145 ("Law"), U.S. Patent App. Pub. 2006/0165060 ("Dua"), and U.S. Patent 6,886,741 ("Salveson").

Law describes a secure wireless authorization system that allows a user to use a wireless device to authorize a third-party transaction request in real time. Law ¶ 47. In Law's system, when an authorization request is received, an authorization server (*i.e.,* a bank) sends an authorization request to the user's wireless device through an encrypted secure channel. *Id.* ¶¶ 36, 49. The channel is encrypted by a pre-established symmetric key, which can be used as a "device password" or "device key." *Id.* ¶¶ 66–67. If the wireless device receives the request, it displays the request to the user and allows the user to respond by inputting a PIN or personal digital signature. *Id.* ¶ 49. If the authorization server receives a response within a certain specified period of time (*i.e.*, a "timeout" period), it confirms that the user's security credentials are correct and allows the transaction to proceed. *Id.* ¶¶ 49–50.

The Board instituted review on all claims and all grounds. After institution, Verify filed a motion to terminate the proceedings, arguing that Askeladden failed to name TCH and Bank of America as real parties in interest as required by 35 U.S.C. § 312(a)(2). The Board determined that TCH should be named as a real party in interest but that neither Bank of America nor any other member banks is in privity with Askeladden or TCH and need not be named. J.A. 611, 614. Rather than terminate the proceedings, the Board allowed Askeladden to update its mandatory notice to name TCH as a real party interest, which it did. J.A. 615, 628. Verify continued to argue that the member banks are real parties in interest in later filings.

Meanwhile, Verify also filed a motion to amend the claims of the '648 patent under 35 U.S.C. § 316(d) in which Verify sought to amend claim 2 and add dependent claims 20–31. J.A. 564–77. Verify later withdrew its proposed addition of claims 20–22 and 26–30. J.A. 730. Askeladden responded that amended claim 2 and new claims 25 and 31 would have been obvious over Law and/or Dua. Askeladden also argued that new claims 23 and 24 lacked written

description support in the specification of the ’648 patent and alternatively that the claims would have been obvious over Law, Dua, and U.S. Patent App. Pub. 2003/0182194 (“Choey”).

The Board issued a final written decision in which the Board determined that Askeladden had demonstrated the unpatentability of claims 1–19 of the ’648 patent, denied Verify’s motion to amend for all claims, and reiterated its conclusion that none of the member banks are real parties in interest to the proceeding. Relevant to this appeal, the Board determined that independent claims 1, 2, and 5, as well as dependent claim 19, would have been obvious over Law and Dua. With respect to Verify’s motion to amend, the Board determined that proposed amended claim 2 and proposed new claims 25 and 31 would have been obvious over Law and Dua and that proposed new claims 23 and 24 would have been obvious over Law, Dua, and Choey. The Board also determined that proposed claims 23 and 24 lack written description support in the specification of the ’648 patent.

Verify appealed. We have jurisdiction under 28 U.S.C. § 1295(a)(4)(A).

DISCUSSION

Verify makes four principal arguments on appeal. First, Verify argues that the Board erred in concluding that the claims would have been obvious over the prior art. Second, Verify argues that the Board erred in denying its motion to amend because the amended claims would have been unpatentable as obvious. Third, Verify argues that the Board erred in determining that Bank of America is not a real party in interest. Finally, Verify argues that the application of *inter partes* review to pre-AIA patents is a taking under the Fifth Amendment. We address Verify’s arguments in turn.

A. Obviousness

Obviousness is a question of law that "lends itself to several basic factual inquiries," *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966) (citing *Great Atl. & Pac. Tea Co. v. Supermarket Equip. Corp.*, 340 U.S. 147, 155 (1950)), including the scope and content of the prior art, the level of ordinary skill in the art, differences between the prior art and the claimed invention, and any relevant secondary considerations. *Id.* "We review the PTAB's factual findings for substantial evidence and its legal conclusions *de novo*." *Redline Detection, LLC v. Star Envirotech, Inc.*, 811 F.3d 435, 449 (Fed. Cir. 2015) (citing *Rambus Inc. v. Rea*, 731 F.3d 1248, 1251 (Fed. Cir. 2013)). A finding is supported by substantial evidence if a reasonable mind might accept the evidence as adequate to support the finding. *Consol. Edison Co. v. NLRB*, 305 U.S. 197, 229 (1938). "If two 'inconsistent conclusions may reasonably be drawn from the evidence in record, the PTAB's decision to favor one conclusion over the other is the epitome of a decision that must be sustained upon review for substantial evidence.'" *Elbit Sys. of Am., LLC v. Thales Visionix, Inc.*, 881 F.3d 1354, 1356 (Fed. Cir. 2018) (quoting *In re Cree, Inc.*, 818 F.3d 694, 701 (Fed. Cir. 2016) (internal brackets omitted)).

1. Claims 1 and 5

Verify argues that the Board erred in concluding that claims 1 and 5 would have been obvious over the prior art. Independent claim 1 recites, *inter alia*, "opening a communications link between the verifier and the user communications device by using the user access number" and "sending an identity verification request (IVR) from the verifier to the user through the communications link." Independent claim 5 recites substantially similar limitations. The Board determined that Law discloses opening a communications channel through its description of connecting an authorization server of the issuing bank (*i.e.*, the verifier) and the user's wireless device. *Decision*, 2018 WL

3572368, at *8. The Board also concluded that Law discloses sending an identification verification request through an open communications link through its description of sending an authorization request from the authorization server to the user's wireless device. *Id*.

Verify argues that the Board improperly failed to construe the term "open[ing] a communications link with the user communications device." Verify further argues that Law fails to disclose the steps of opening a communications channel and sending an IVR through the channel because the authorization server of Law transmits its authorization request to the user's wireless device through a third-party intermediary without having previously opened a communications channel with the user's device. Verify also challenges the Board's finding of a motivation to combine Law with Dua.

Askeladden responds that Verify's claim construction argument is waived because Verify failed to seek construction of any claim terms before the Board and that the Board's conclusion that Law discloses opening a communications link is supported by substantial evidence, including the testimony of its expert, Ivan Zatkovich.

We agree with Askeladden on both counts. Verify did not file a preliminary response to Askeladden's petition for *inter partes* review, and the Board, in its institution decision, determined that no claim terms required construction. *Askeladden LLC v. Verify Smart Corp.*, No. IPR2017-00726, Paper 6 at 7 (P.T.A.B. July 24, 2017). Thereafter, Verify failed to request or propose a construction for any claim terms in its patent owner's response. *See Askeladden LLC v. Verify Smart Corp.*, No. IPR2017-00726, 2017 WL 6061669 (P.T.A.B. Nov. 20, 2017). Having failed to present its claim construction argument before the Board, Verify is not entitled to present that argument for the first time on appeal. *See In re Baxter Int'l*, 678 F.3d 1357, 1362 (Fed. Cir. 2012) ("Absent exceptional circumstances, we

generally do not consider arguments that the applicant failed to present to the Board." (internal citations omitted)).

Under the plain and ordinary meaning of the claim terms as adopted by the Board, we agree with Askeladden that the Board's finding that Law discloses opening a communications channel and sending an IVR through the channel is supported by substantial evidence. Before the Board, Verify argued that Law's authorization system operates using an SMS (short message service) network, in which communications from the authorization server to the user's wireless device are routed through an SMSC (short message service center), which is operated by the wireless carrier, not the bank. J.A. 377–80. According to Verify, at the time that the authorization server transmits the authorization request to the SMSC, no communications link is open with the user's device. J.A. 384. In response, relying on the declaration of Zatkovich, Askeladden argued that Law's authorization server establishes an encrypted communications channel with the user device and subsequently transmits its authorization request to the user's device through this channel.

Having been presented with competing theories as to how Law's authorization server communicates with the user's wireless device, the Board found that Law discloses the claimed communications link. Our task is not to determine which theory we find more compelling. "[I]t is not for us to second-guess the Board's assessment of the evidence." *Velander v. Garner*, 348 F.3d 1359, 1378 (Fed. Cir. 2003). Rather, the only question before us is whether the finding adopted by the Board is supported by substantial evidence. Here, we conclude that it is.

Zatkovich testified that, in his opinion, Law's authorization server "opens a 'communications link' prior to sending a message." J.A. 3283 ¶ 150. This testimony accords with the disclosure of Law, which explains that, if a

transaction is not pre-authorized, then the authorization server will "attempt to connect to the wireless device." Law ¶ 62. Thereafter, if the user's device is available, then the authorization server will "send out an authorization request" to the user's wireless device "through an encrypted secure channel . . . connecting the authorization server and the user's wireless device." *Id*. With respect to Verify's argument that use of SMS precludes establishing a communications link between the authorization server and the user's device, Zatkovich testified that Law discloses establishing a secure wireless connection between an authorization server and the user communications device "irrespective of the protocol selected," such as SMS. J.A. 3285 ¶ 153. The disclosure of Law comports with Zatkovich's testimony that Law's encrypted channel can support various communication protocols. As Law explains, the user's wireless device "must handle various security schemes and communication channels." Law ¶ 70. Based on Law's disclosure and Zatkovich's testimony, we conclude that the Board's finding that Law discloses opening a communications link between the verifier (Law's authorization server) and the user communication device, as well as sending an identity verification request (Law's authentication request) from the verifier to the user through the communications link is supported by substantial evidence.

Substantial evidence also supports the Board's finding of a motivation to combine Law with Dua. The Board credited Zatkovich's testimony that a skilled artisan would have been motivated to combine Law with Dua because the references "are both directed to electronic transaction processing and, in particular, verifying and authenticating users and authorizing financial transactions." J.A. 988 ¶ 54. Zatkovich further testified that a person of skill would have recognized that combining Law with Dua would facilitate "the convenience and flexibility offered by over-the-air, on demand, download methods." J.A. 993 ¶ 64. Accordingly, we affirm the Board's finding of a motivation to combine

the references, and hence the obviousness of claims 1 and 5.

2. Claim 19

Claim 19 depends from claim 5 and recites the additional steps of storing a "device identifier" of the user communications device in the database, obtaining the device identifier of the user communications device used during verification, comparing the device identifier obtained during verification with the device identifier stored in the database, and, if the device identifiers match, allowing the transaction. '648 patent col. 22 ll. 16–28. The Board determined that "device keys" described in Law to encrypt messages sent through Law's secure encrypted channel disclose the device identifier recited in claim 19, and that Law discloses the remaining steps of claim 19 through its description of verifying the device credentials of the user's device prior to authorizing a transaction. *Decision*, 2018 WL 3572368, at *11.

Verify argues that Law's use of device keys to encrypt communication does not meet the limitations of claim 19 because, while the device keys may be used to verify the credentials of the user's device, the key is never transmitted to the authorization server and compared to an identifier stored in the server, as required by the claim. Askeladden responds that substantial evidence supports the Board's conclusion that Law's device keys disclose a device identifier and are used in the manner recited in the claim.

We agree with Askeladden. Law explains that the symmetric key used to encrypt communications between the authentication server and user device "can be used as a device password" or "device key." Law ¶ 67. Further, "[u]pon receiving the response from the wireless device, the authorization server will . . . verify the security credentials of the user and the wireless device." Law ¶ 50. In reaching its conclusion that Law discloses comparing the device key

with a key stored in the authorization server, the Board credited Zatkovich's testimony that a skilled artisan "would have understood that verifying the separate security credentials of the wireless device requires retrieving and comparing the stored value of these credentials . . . to that retrieved from the user communication device." J.A. 3294 ¶ 171. The Board was within its discretion to weigh the credibility of expert testimony, *see Yorkey v. Diab*, 601 F.3d 1279, 1284 (Fed. Cir. 2010) (citing *Velander*, 348 F.3d at 1371), and Verify has not otherwise demonstrated that the Board's finding is unsupported by substantial evidence, or that claim 19 was not obvious.

B. Motion to Amend

Verify argues that the Board erred in denying its motion to amend the claims under 35 U.S.C. § 316(d). We address the challenged amendments and proposed new claims in turn.

1. Claims 2, 25, and 31

Independent claim 2 recites substantially similar subject matter as claim 1. In its motion to amend, Verify sought to amend claim 2 additionally to recite "wherein the first verifier communication device is configured to open a communication link with the user communications device, and thereafter determine whether the open communication link has been broken." J.A. 566. Verify also proposed to amend claim 2 to further limit the condition in which the transaction proceeds to require that "the open communications link is not previously broken." J.A. 566–67. Proposed dependent claims 25 and 31 similarly require that the transaction is blocked if the opened communication link is broken. J.A. 575, 577. The Board determined that Law's timeout feature discloses the proposed limitations that the verifier determine whether the communication link is broken and that the transaction is made contingent on a determination that it is not. *Decision*, 2018 WL 3572368, at *20. Accordingly, the Board concluded that the proposed

amendments are unpatentable as obvious over the prior art.

Verify argues that Law does not disclose the amended limitations because Law's timeout feature only indicates the failure of a user to respond within a predetermined amount of time and does not indicate whether the communications link is broken. Askeladden responds that the Board's conclusion was supported by substantial evidence.

We agree with Askeladden. Law explains that "[i]n the event that the user does not respond to the request within the specified time limit, the authorization server will . . . deny the request or wait for the postauthorization model to take effect . . . ." Law ¶ 63. Zatkovich testified that a person of skill would have understood that "a 'broken' communication link would include a link where the line is 'dropped' or a response is not received within a specified time period." J.A. 3304 ¶ 192. Indeed, the '648 patent itself describes a communications link being "timed-out" as one example of when the link is "broken." '648 patent col. 8 ll. 28–32. Accordingly, we conclude that the Board's determination that amended claim 2 and proposed new claims 25 and 31 would have been obvious over the prior art is supported by substantial evidence, and that the motion to amend was properly denied.

2. Claims 23 and 24

Proposed claim 23 depends from claim 5 and further recites "determining a location of the user communications device with a GPS locating function on a cell phone." J.A. 574. Proposed claim 24 includes the same limitation by virtue of its dependency on claim 23. The Board determined that the proposed claims lack written description support in the specification because, while the specification of the '648 patent provides written description support for determining a location of a cell phone via a GPS locating function, it does not provide support for determining a location of other types of devices encompassed by the user

communication device. *Decision*, 2018 WL 3572368, at *19. Alternatively, the Board concluded that the proposed claims would have been obvious over Law, Dua, and Choey. *Id*. at *21. Accordingly, the Board denied Verify's motion to add claims 23 and 24.

Verify argues that under the broadest reasonable interpretation proposed claims 23 and 24 require only that the GPS elements of a locating function must be on the recited cell phone, not the communications device itself, which is supported by the specification. Further, Verify argues that the Board's conclusion that the claims would have been obvious over the prior art is unsupported by substantial evidence because Choey describes a system in which the GPS receivers are located on top of cell towers, not "on a cell phone," as required by the claims.

Askeladden responds that the Board correctly determined that the proposed claims lack written description support because the claims recite determining the location of a communications device, and the specification only describes how to determine the location of a cell phone. Even if the specification provides written description support for the claims, Askeladden argues, the Board's conclusion that Choey discloses using a GPS-enabled mobile phone system to detect mobile phone location was supported by substantial evidence.

We agree with Askeladden and the Board that Verify's proposed claims improperly introduce new matter. Proposed amendments "may not enlarge the scope of the claims of the patent or introduce new matter." 35 U.S.C. § 316(d)(3). The passage on which Verify relies for support of its replacement claims recites: "[B]ecause of the GPS locating functions now universal on cell phones, any attempted false verification query can automatically trigger a tracking routine to immediately locate the stolen cell phone." '648 patent col. 5 ll. 30–33. But the written description explains that the term "communications device"

as used in the '648 patent "is intended broadly to include communications devices of any nature linked in a communications system," including computers. *Id.* col. 2 ll. 21–27. Thus, while the written description discloses determining the location of cell phones, the proposed claims recite determining the location of other types of devices. Even under Verify's reading of the claims in which only the GPS function is on a cell phone, the written description does not disclose using the cell phone to track devices other than the cell phone—specifically, the user communications device. Accordingly, we agree that proposed claims 23 and 24 introduce new matter and affirm the Board's denial of Verify's motion to amend as to those claims.

Having affirmed the Board's conclusion that proposed claims 23 and 24 introduce new matter to the specification of the '648 patent, we need not address the Board's decision that those claims would have been obvious over the prior art.

C. Real Party in Interest

Verify argues that the Board erred in concluding that Bank of America is not a real party in interest. According to Verify, Bank of America should be named as a real party in interest in the proceedings because of the member banks' control over TCH. Because Verify asserted the '648 patent against Bank of America more than one year before Askeladden filed its petition for *inter partes* review, Verify argues that Askeladden's petition should be dismissed as time-barred under 35 U.S.C. § 315(b).

Verify's argument is foreclosed by intervening precedent. In *Thryv, Inc. v. Click-To-Call Techs., LP*, the Supreme Court held that 35 U.S.C. § 314(d) precludes judicial review of the Board's application of the one-year time bar set forth in § 315(b). 140 S. Ct. 1367 (2020). The Court explained that "a contention that a petition fails under § 315(b) is a contention that the agency 'should have refused to institute an *inter partes* review,'" and therefore a

challenge to a petition's timeliness under § 315(b) is a dispute about the application of an institution-related statute and is barred from appellate review by § 314(d). *Id.* at 1373–74 (quoting 35 U.S.C. § 314(d)).

Thereafter, in view of *Click-To-Call*, this court held that preclusion of judicial review under § 314(d) "extend[s] to a Board decision concerning the 'real parties in interest' requirement of § 312(a)(2)." *ESIP Series 2, LLC v. Puzhen Life USA, LLC*, 958 F.3d 1378, 1386 (Fed. Cir. 2020). Accordingly, we hold that § 314(d) precludes our review of the Board's decision that Bank of America is not a real party in interest.

Somewhat relatedly, Verify also argues that the operation of TCH by the member banks is an unlawful restraint of trade under the Sherman Act. Observing that it lacks jurisdiction to determine Sherman Act violations, the Board declined to address Verify's argument. *Decision*, 2018 WL 3572368, at *15 n.6. The proceedings that may be addressed by the Board are enumerated by statute. *See* 35 U.S.C. § 6(b)(1)–(4). Relevant here, the scope of *inter partes* review is limited to requests to cancel claims of issued patents as unpatentable under 35 U.S.C. §§ 102 and 103 and does not extend to alleged antitrust violations. 35 U.S.C. § 311(b). Accordingly, we agree with the Board that it lacked jurisdiction to address Verify's antitrust allegations in the first instance and similarly decline to address Verify's arguments on appeal.

D. Takings Claim

Finally, Verify argues that the retroactive application of *inter partes* review to patents that issued prior to the enactment of the America Invents Act ("AIA") is a taking under the Fifth Amendment, but Verify's argument is foreclosed by our precedent. In *Celgene Corp. v. Peter*, we held that "the retroactive application of IPR proceedings to pre-AIA patents is not an unconstitutional taking under the Fifth Amendment." 931 F.3d 1342, 1362 (Fed. Cir.

2019). Accordingly, we hold that the retroactive application of IPR proceedings to the '648 patent, which issued before the enactment of the AIA, is not an unconstitutional taking.

We note briefly that Verify also raises due process challenges to various procedural decisions of the Board. Specifically, Verify argues that the Board violated due process by denying Verify's request for discovery from TCH for evidence of secondary considerations of nonobviousness and the member banks' status as real parties in interest. We review the Board's application of its rules for trial proceedings for abuse of discretion. *Ultratec, Inc. v. CaptionCall, LLC*, 872 F.3d 1267, 1271–72 (Fed. Cir. 2017); *Redline Detection*, 811 F.3d at 442. In denying Verify's request, the Board observed that "TCH has not entered any papers or testimony in this proceeding. Nor has TCH advanced any positions during this proceeding" and that 37 C.F.R. § 42.51(b)(1)(iii) requires routine discovery of only "relevant information that is inconsistent with a position advanced by *the* party." J.A. 648 (emphasis in original). Since TCH had not advanced any position in the proceeding, the Board determined that it was not subject to routine discovery. In any event, the Board also determined that Verify's requests were untimely. We find that the Board's determination that Verify's motions were overbroad and untimely was reasonable and that the Board did not abuse its discretion in denying the motions.

CONCLUSION

We have considered Verify's remaining arguments but find them unpersuasive. For the foregoing reasons, the decision of the Board is affirmed.

AFFIRMED