UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS INC.,
Petitioner,

v.

VINDOLOR, LLC,
Patent Owner.

Case IPR2019-00478
Patent 6,213,391 B1

Before KALYAN K. DESHPANDE, WILLIAM V. SAINDON,
and SCOTT E. BAIN, *Administrative Patent Judges*.

SAINDON, *Administrative Patent Judge*.

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

I. INTRODUCTION

Unified Patents, Inc. (“Petitioner”) filed a petition requesting *inter partes* review of claims 1 and 2 of U.S. Patent No. 6,213,391 B1 (Ex. 1001, “the ’391 patent”). Paper 1 (“Pet.”). Vindolor, LLC (“Patent Owner”) filed a Preliminary Response. Paper 6 (“Prelim. Resp.”).

We have authority under 35 U.S.C. § 314, which provides that an *inter partes* review may not be instituted unless the information presented in the Petition and the Preliminary Response shows that “there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314; *see also* 37 C.F.R. § 42.4(a) (“The Board institutes the trial on behalf of the Director.”). Taking into account the arguments presented in the Petition and Preliminary Response, we conclude that the information presented in the Petition does not establish a reasonable likelihood that Petitioner would prevail with respect to at least one challenged claim. Accordingly, we do not institute an *inter partes* review.

A. Related Matters

According to the parties, the ’391 patent is involved in 11 district court proceedings. Pet. 1–2; Paper 4, 2–3.

The parties do not report any related USPTO proceedings.

B. The ’391 Patent

The ’391 patent is directed to a system for identifying an individual using biometric characteristics of that person. Ex. 1001, Abstract. One embodiment takes the form of a card similar to an ATM card. *See id.* at 4:58–62, 7:35–40. In use, biometric characteristics are captured from the user to generate an identification profile representing the biometric input. *Id.* at 3:66–4:2. Then, the identification profile is used to calculate an access code. *Id.* at 4:13–17. In summary, the device disclosed in the '391 patent receives biometric information from an input, converts that biometric information into an identification profile, and then applies an algorithm to the identification profile to generate an access code.

C. Challenged Claims

Claims 1 and 2 are challenged, and are the only claims in the patent. Independent claim 1 is reproduced below (carriage returns added for readability):

> 1. A portable identification system comprising
> a storage medium for storing electronic data;
> one or more inputs;
> one or more outputs;
> a verifying means for determining user authorization or non-authorization,
> said verifying means receiving data from at least one of said one or more inputs, which data is derived from biometric or other distinctive characteristics of the user,
> said verifying means generating an identification profile for each user, wherein said identification profile is determined from said data, and
> a code generator employing at least one code generating algorithm for generating one or more access codes based upon said identification profile wherein at least one of the said one or more access codes is an identification specific digital signature.

D. Prior Art and Asserted Grounds

Petitioner raises the following prior art challenges:

Reference(s)	**Basis**	**Claims Challenged**
Gullman[1]	§ 102	1 and 2
Gullman	§ 103	1 and 2
Lane[2] and Drexler[3]	§ 103	1 and 2

II. PATENTABILITY ANALYSIS

A. Claim Construction

We construe claims in an *inter partes* review using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. § 282(b). 37 C.F.R. § 42.100(b). Accordingly, we will apply a district-court type claim construction in this proceeding.

Petitioner provides a construction for the "verifying means" of claim 1. Pet. 21–26. Patent Owner does not contest Petitioner's construction directly, but instead points out some nuances it believes exist when considering the term. Prelim. Resp. 18–19 ("the verifying means must receive data *from* the one or more inputs then generate an identification profile from [that data]"). For the purposes of this Decision, we are persuaded by Petitioner, and, accordingly, adopt Petitioner's construction.

[1] U.S. Patent No. 5,280,527, issued Jan. 18, 1994 (Ex. 1004).

[2] U.S. Patent No. 5,623,552, issued Apr. 22, 1997 (Ex. 1005).

[3] U.S. Patent No. 5,457,747, issued Oct. 10, 1995 (Ex. 1006).

No other claim terms require construction at this time. *See, e.g.*, *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) ("[W]e need only construe terms 'that are in controversy, and only to the extent necessary to resolve the controversy.'") (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

B. Level of Ordinary Skill in the Art

Petitioner asserts the following level of ordinary skill in the art:

> A person of ordinary skill in the art . . . would have had at least a Bachelor's degree in Computer Science, Computer Engineering, or Electrical Engineering, and two to three years of experience with user identification/authentication systems or cards (devices), including the use of biometric information. (Ex-1002, ¶¶67-70). More work experience could substitute for education, and vice versa. (Ex-1002, ¶¶67-70)

Pet. 20.

Patent Owner states that it "does not contest Petitioner's assertion." Prelim. Resp. 6. Accordingly, we adopt Petitioner's proposed level of skill for purposes of this Decision.

C. The Gullman Anticipation Ground

Gullman discloses a security access device that uses a person's biometric characteristics in order to determine whether access should be given. Ex. 1004, Abstract. The security access device could be in a form similar to a credit card, and may be capable of reading biometric information from a holder of that card, such as a fingerprint.[4] *Id.* at 5:34–50. In

[4] Although other forms of biometric input are specified in Gullman (*see* Ex. 1004, 2:29–30), for sake of illustration we will refer only to fingerprints.

operation, a template of the authorized user's fingerprint is stored on the card. *Id.* at 2:27–30. Then, when a user wishes to access a system using the card, she provides her fingerprint on the card, which then compares the received fingerprint to the authorized users' template in order to determine a correlation factor. *Id.* at 3:44–46. The card then bundles the correlation factor and another code (e.g., a PIN, embedded serial number, or account number) into a security token. *Id.* at 4:3–8. The security token is sent to a host computer to determine if access should be granted—it decodes the security token to review the correlation factor and the other code. *Id.* at 4:13–15. A threshold correlation factor determines if the stored and provided fingerprints are sufficiently similar to permit access (in conjunction with the other code). *Id.* at 3:45–47, 6:13–22.

Petitioner asserts that Gullman anticipates the subject matter of claims 1 and 2. Pet. 26–44. In relevant part to this Decision, Petitioner asserts that Gullman's security token is the access code of claim 1. *Id.* at 43. According to claim 1, the access code is based on an identification profile and is an identification specific digital signature.

Patent Owner argues, and we agree, that Gullman's security token is not an access code because the security token is used to provide transmission security, not to provide access. Prelim. Resp. 42–44. Indeed, Gullman highlights the functional difference between something used to provide access and something used to provide security: "[a] PIN is used to identify an individual and authorize access to a host system," which "provides user identification, while a token provides transmission security." Ex. 1004, 1:30–45. Gullman decodes the security token and uses what is encoded within to determine whether to grant access. *Id.* at 4:13–15 ("The access device 12 sends the token to the host 10 which decodes the token to identify the embedded fixed code and correlation factor.”); *see also id.* at 4:29–31, 6:39–45. Thus, the security token in Gullman provides transmission security, whereas the data contained within (the correlation factor and the code) are used to authorize access. Because we are not persuaded that Gullman discloses an access code in the claimed manner, we are not persuaded that there is a reasonable likelihood that Gullman anticipates claim 1, or claim 2 which depends therefrom.

D. The Gullman Obviousness Ground

Petitioner’s Gullman obviousness ground adds nothing new to the access code limitation; for that limitation, Petitioner refers us back to its anticipation ground. *See* Pet. 47–48 (“Gullman alone discloses or at least renders obvious [the access code limitation] based on the same intrinsic and extrinsic evidence and reasoning described in [the Gullman anticipation ground].”). Thus, this ground does not establish a reasonable likelihood of success for the same reasons as the Gullman anticipation ground.

E. The Lane-Drexler Obviousness Ground

Petitioner asserts that claims 1 and 2 would have been obvious in view of Lane and Drexler. Pet. 49–81. Lane discloses a self-authenticating identification card that uses a fingerprint sensor to determine if the card holder is an authorized user. *See* Ex. 1005, Abstract, 2:29–35. Fingerprint information regarding an authorized user is stored on the card. *Id.* at 2:64–3:8. When a user tries to authenticate using the card, the card will read her fingerprint and compare it with the stored fingerprint information. *Id.* at 2:29–35. If the user’s fingerprint and the stored fingerprint match, then an authentication signal is provided, which may be visual, audio, or in the form of a programmable magnetic stripe code. *Id.* at 3:55–65.

Structurally, the Lane device operates by using a fingerprint sensor in conjunction with an authenticator or controller. *See generally id.* at Fig. 2. The fingerprint sensor is a two-dimensional array of ridge detectors. *Id.* at 7:9–16. Each ridge detector has a small processor, and the array of such processors form a parallel processing network to collectively arrive at a pixel array that identifies relevant landmarks in a fingerprint. *See generally id.* at 7:17–8:30. Once the fingerprint sensor provides the relevant fingerprint data, the authenticator or controller in Lane compares that data to the stored fingerprint data to determine if the user is authorized. *Id.* at 5:37–46 (authenticator described as performing the function); 8:30–32 (controller described as performing the function). The authentication signal, if in audio form, may be "a predetermined coded audio signal," but no further detail is provided. *See id.* at 9:1–15.

Petitioner's ground specifies that Lane's authenticator generates the claimed identification profile when it creates a two-dimensional binary image of the fingerprint. Pet. 77 ("In Lane, authenticator 107 uses 'information related to a sensed fingerprint' . . . to create a 'two dimensional binary image' (*i.e.*, ***generating an identification profile***) of a fingerprint's pattern.").

But as Patent Owner argues, and we agree, Lane's authenticator does not generate a two-dimensional binary image of the fingerprint. Prelim. Resp. 53–57. Although Petitioner asserts that the authenticator "create[s] a 'two dimensional binary image,'" Petitioner cites to a passage that is discussing how the *fingerprint sensor* works, not the authenticator.

Compare Pet. 77 (citing Ex. 1005, 7:14–20) *with* Ex. 1005, 7:14–20 (talking about the functions of the ridge detectors 140 of the fingerprint sensor). Accordingly, we are not persuaded by Petitioner's assertion that Lane discloses a verifying means that generates an identification profile in the form of a two dimensional binary image. For that reason, we are not persuaded that Petitioner has demonstrated a reasonable likelihood that claims 1 or 2 are unpatentable over Lane and Drexler.

III. ORDER

In view of the foregoing, it is hereby ORDERED that Petitioner's request for *inter partes* review of the '391 patent is denied.

For Petitioner:

Cono Carrano
ccarrano@akingump.com

Ashraf Fawzy
afawzy@unifiedpatents.com

Jung S. Hahm
jung@unifiedpatents.com

For Patent Owner:

Raymond Mort
raymort@gmail.com

Cabrach Connor
cab@connorleepllc.com