NOTE: This disposition is nonprecedential.

United States Court of Appeals for the Federal Circuit

DYNAPASS IP HOLDINGS LLC,
Plaintiff-Appellant

v.

BANK OF AMERICA CORPORATION, BANK OF AMERICA, N.A.,
Defendants-Appellees

2025-1222

Appeal from the United States District Court for the Eastern District of Texas in No. 2:22-cv-00210-JRG-RSP, Judge J. Rodney Gilstrap.

Decided: June 11, 2026

FRED WILLIAMS, Williams Simons and Landis PC, Austin, TX, argued for plaintiff-appellant. Also represented by STEPHEN ROGER DARTT.

EIMERIC REIG-PLESSIS, Winston Taylor LLP, San Francisco, CA, argued for defendants-appellees. Also represented by DUSTIN JAMES EDWARDS, WILLIAM LOGAN, Houston, TX; CLAIRE A. FUNDAKOWSKI, Washington, DC.

Before MOORE, *Chief Judge*, CHEN, *Circuit Judge*, and BISSOON, *Chief District Judge*.[1]

MOORE, *Chief Judge*.

Dynapass IP Holdings LLC (Dynapass) appeals the United States District Court for the Eastern District of Texas' order dismissing with prejudice Dynapass' claim that Bank of America Corporation and Bank of America, N.A. (BOA) infringe U.S. Patent No. 6,993,658. For the following reasons, we *affirm*.

BACKGROUND

Dynapass owns the '658 patent, which relates to systems and methods for user authentication in which user tokens are supplied through communication devices. '658 patent at 1:1–7. The system authenticates users using a password, which is based on a passcode and a token. *Id.* at 4:36–65. Claim 1 is representative:

> 1. A method of authenticating a user on a first secure computer network, the user having a user account on said first secure computer network, the method comprising:
>
> associating the user with a personal communication device possessed by the user, said personal communication device in communication over a second network, wherein said second network is a cell phone network different from the first secure computer network;

[1] Honorable Cathy Bissoon, Chief District Judge, United States District Court for the Western District of Pennsylvania, sitting by designation.

> receiving a request from the user for a token via the personal communication device, over the second network;
>
> *generating a new password* for said first secure computer network *based at least upon the token and a passcode*, wherein the token is not known to the user and wherein the passcode is known to the user;
>
> *setting a password* associated with the user *to be the new password*;
>
> activating access the user account on the first secure computer network;
>
> transmitting the token to the personal communication device;
>
> *receiving the password from the user* via the first secure computer network; and
>
> deactivating access to the user account on the first secure computer network within a predetermined amount of time after said activating, such that said user account is not accessible through any password, via said first secure computer network.

Id. at 11:43–12:13 (emphases added).

Dynapass sued BOA, accusing the two-factor authentication feature of BOA's Mobile Banking Application of infringing claims 1–7 of the '658 patent. J.A. 116–24. Based on the district court's construction of "receiving the password," J.A. 17–19, the parties filed a Joint Stipulation of Non-Infringement and Motion for Entry of Final Judgment, J.A. 943–48. The district court treated the motion as a motion for dismissal and dismissed the case with prejudice. J.A. 955. Dynapass appeals. We have jurisdiction under 28 U.S.C. § 1295(a)(1).

DISCUSSION

We review a district court's claim construction based on intrinsic evidence de novo and review any findings of fact regarding extrinsic evidence for clear error. *Speed-Track, Inc. v. Amazon.com*, 998 F.3d 1373, 1378 (Fed. Cir. 2021) (citation omitted).

Dynapass argues the district court erred in construing "receiving the password" in claim 1[2] to preclude separate receipt of the "passcode" and "token" components of the password. Appellant's Br. 23–36; *see* J.A. 17–19. Specifically, Dynapass argues the district court limited "receiving the password" to the preferred embodiment where "the user 108 combines the passcode 154 and the token to form a password" and improperly excluded an alternative embodiment where "the passcode 154 and the token 156 are submitted separately." Appellant's Br. 32–34; '658 patent at 4:52–61. We do not agree.

While the written description discloses multiple embodiments for authenticating a user, the patentee's chosen claim language unambiguously does not extend to the alternative embodiment where the passcode and token are received separately. *TIP Sys., LLC v. Phillips & Brooks/Gladwin, Inc.*, 529 F.3d 1364, 1373 (Fed. Cir. 2008) ("[T]he mere fact that there is an alternative embodiment disclosed in the [asserted] patent that is not encompassed by district court's claim construction does not outweigh the language of the claim, especially when the court's construction is supported by the intrinsic evidence."). Claim 1 recites (1) "generating a new password . . . based at least upon the token and a passcode;" (2) "setting a password . . . to be the new password;" and then (3) "receiving the password from the user . . . ." This language requires

---

[2] Independent claim 5 similarly recites "receive the password." '658 patent at 12:20–48.

generating a password from the passcode and token before receiving the password. Receiving the passcode and token separately would not constitute "receiving the password" since the individual passcode and token components are not the claimed "password."

The written description supports this construction. In the alternative embodiment, the written description never refers to separate reception of the passcode and token as receiving the *password*. '658 patent at 4:59–61 ("In an alternative embodiment, the passcode 154 and the token 156 are submitted separately."). The written description also repeatedly juxtaposes the password with the passcode and token components. *See e.g.*, '658 patent at 5:8–10 (describing authenticating a user based on "a supplied password 158 or a passcode 154 and a token 156 combination"); 5:18 (juxtaposing "password data" with "passcode and token data"); 7:41–45 ("In the preferred embodiment, the user 108 combines the passcode 154 and the token 156 by concatenation to form the password 158. In an alternative embodiment, the passcode 154 and the token 156 are submitted separately."). This repeated and consistent juxtaposition between the password and its requisite components confirms that separately receiving the passcode and token does not constitute "receiving the password." *GPNE Corp. v. Apple Inc.*, 830 F.3d 1365, 1370 (Fed. Cir. 2016) ("We have recognized that when a patent repeatedly and consistently characterizes a claim term in a particular way, it is proper to construe the claim term according to that characterization.") (internal quotation and citation omitted). We see no error in the district court's construction of "receiving the password" to preclude separate reception of the passcode and token.

CONCLUSION

We have considered Dynapass' remaining arguments and find them unpersuasive. Because the district court did not err in construing "receiving the password," we *affirm*.

AFFIRMED

COSTS

Costs to BOA.