

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS, LLC,
Petitioner,

v.

DYNAPASS IP HOLDINGS LLC,
Patent Owner.

IPR2023-00425
Patent 6,993,658 B1

Before KEVIN F. TURNER, KRISTEN L. DROESCH, and
LYNNE H. BROWNE, *Administrative Patent Judges*.

BROWNE, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314, 37 C.F.R. § 42.4

I. INTRODUCTION

Unified Patents, LLC (“Petitioner”) filed a Petition (Paper 1 (“Pet.”)) requesting institution of an *inter partes* review of claims 1 and 3–6 of U.S. Patent No. 6,993,658 B1 (Ex. 1001, “the ’658 Patent”). Dynapass IP Holdings LLC (“Patent Owner”) timely filed a Preliminary Response. Paper 8 (“Prelim. Resp.”).

Under 35 U.S.C. § 314(a), an *inter partes* review may not be instituted unless the information presented in the Petition and any response thereto shows “there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” Upon consideration of the Petition and the evidence of record, we conclude that the information presented in the Petition establishes that there is a reasonable likelihood that Petitioner would prevail in challenging at least one of claims 1 and 3–6 of the ’658 Patent as unpatentable under the grounds presented in the Petition. Pursuant to § 314, we hereby institute an *inter partes* review as to the challenged claims of the ’658 Patent.

A. *Real Parties in Interest*

Petitioner identifies itself, Unified Patents, LLC, as the only real party-in-interest. Pet. 79. Patent Owner identifies itself, Dynapass IP Holdings LLC and DynaPass Inc., as the only real parties-in-interest. Paper 3, 1.

B. *Related Matters*

The parties identify the following as related district court matters: *Dynapass IP Holdings LLC v. Regions Financial Corporation*, 2:22-cv-00215 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. JPMorgan Chase & Co.*, 2:22-cv-00212 (EDTX 6-17-2022), *Dynapass IP Holdings LLC*

IPR2023-00425
Patent 6,993,658 B1

v. PlainsCapital Bank, 2:22-cv-00213 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. Woodforest National Bank*, 2:22-cv-00218 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. Bank of America Corporation*, 2:22-cv-00210 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. Wells Fargo & Company*, 2:22-cv-00217 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. Truist Financial Corporation*, 2:22-cv-00216 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. PNC Financial Services*, 2:22-cv-00214 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. BOKF, National Association*, 2:22-cv-00211 (EDTX 6-17-2022), *Dynapass Inc. v. Mobile Authentication Corporation*, 8:18-cv-01173 (C.D. Cal. 7-3-2018). Pet. 80–81; Paper 3, 1–2.

Patent Owner also identifies *Bank of America, N.A. v. Dynapass IP Holdings LLC*, IPR2023-00367 (filed January 3, 2022) as a related matter. Paper 3, 2.

C. The '658 Patent

The '658 Patent is titled “Use of Personal Communication Devices For User Authentication.” Ex. 1001, code (54). The invention “relates generally to the authentication of users of secure systems and, more particularly, the invention relates to a system through which user tokens required for user authentication are supplied through personal communication devices such as mobile telephones and pagers.” *Id.* at 1:7–11.

One embodiment of the invention provides a password setting system that includes a user token server and a communication module wherein a user token server generates a random token in response to a request for a new password from a user. Ex. 1001, 1:63–2:2. “The server creates a new

password by concatenating a secret passcode that is known to the user with the token” and “sets the password associated with the user’s user ID to be the new password.” *Id.* at 2:2–6. A “communication module transmits the token to a personal communication device, such as a mobile phone or a pager carried by the user.” *Id.* at 2:6–8. Then, the user concatenates the secret passcode with the received token in order to form a valid password, which the user submits to gain access to the secure system. *Id.* at 2:8–11.

Figure, reproduced below, “illustrates an overview, including system components, of a user authentication system 100 according to a preferred embodiment of the present invention.” Ex. 1001, 4:2–4.

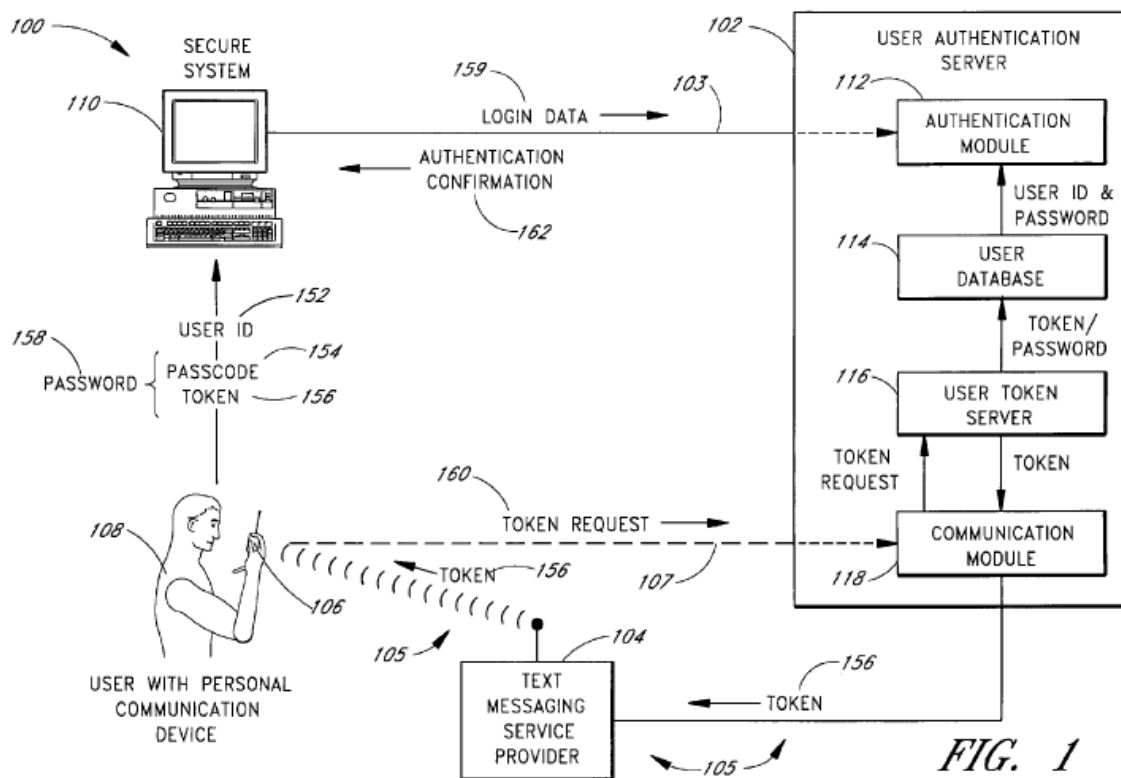


FIG. 1

User authentication system 100 includes authentication Server 102, text messaging Service provider 104, personal communication device 106 carried

by user 108, and secure system 110 to which the authentication system 100 regulates access. *Id.* at 4:9–13. “[P]ersonal communication device 106 is preferably a pager or a mobile phone having SMS (short message Service) receive capability.” *Id.* at 4:13–15. Secure system 110 can be “any system, device, account, or area to which it is desired to limit access to authenticated users.” *Id.* at 4:18–20.

User authentication server 102 is configured to require that user 108 supply authentication information through secure system 110 in order to gain access to secure system 110. Ex. 1001, 4:32–35. Authentication information provided by the user includes user ID 152, passcode 154 and user token 156. *Id.* at 4:36–37. User ID 152 may be publicly known and used to identify the user and passcode 154 is secret and only known to the user 108, whereas token 156 is provided only to user 108 by user authentication server 102 through personal communication device 106. *Id.* at 4:39–44. To gain access to secure system 100, user 108 combines token 156 with passcode 154 to form password 158. *Id.* at 4:52–53. Thus, user 108 needs to have personal communication device 106 in order to gain access to secure system 110. *Id.* at 4:46–48. Further, token 156 has a limited lifespan, such as 1 minute or 1 day. *Id.* at 4:44–45.

D. Challenged Claims

Petitioner challenges claims 1 and 3–6. Pet. 1. Claims 1 and 5, reproduced below with Petitioner’s identifiers included, are the independent claims at issue in this proceeding. Ex. 1001, 11:43–12:13, 12:20–47. Claims 3 and 4 depend from claim 1 and claim 6 depends from claim 5. *Id.* at 12:16–19, 12:48–52.

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.