IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

DYNAPASS IP HOLDINGS LLC,	§	
	§	
Plaintiff,	§	CIVIL ACTION NO. 2:22-cv-00212-JRG-RSP
	§	(Lead Case)
v.	§	
	§	
JPMORGAN CHASE & CO., et al,	§	
	§	
Defendants.	§	

CLAIM CONSTRUCTION ORDER

In these consolidated patent cases, Dynapass IP Holdings LLC alleges infringement by Defendants of various claims of U.S. Patent No. 6,993,658. The patent "relates to a system through which user tokens required for user authentication [for a secure computer system] are supplied through personal communication devices such as mobile phones and pagers." '658 Patent at 1:8–11.

The parties dispute the scope of five terms. For each term, Dynapass alleges a "plain and ordinary meaning" construction, whereas Defendants propose specific language. Having considered the parties' briefing and arguments of counsel during the October 5, 2023 hearing, the Court resolves the disputes as follows.

I. BACKGROUND

The patent addresses a problem with the traditional use of a user ID and password for user authentication to a computer system. According to the patent:

> Guessing passwords is a frequent technique used by "hackers" to break into systems. Therefore, many systems impose regulations on password formats that require mixtures of letters of different cases and symbols and that no part of a password be a word in the dictionary. A user's inability to remember complex combi-

nations of letters, numbers, and symbols often results in the password being written down, sometimes on a note stuck to the side of a workstation.

Present systems face several problems: users dread frequent password changes, [and] frequent password changes with hard-to-remember passwords inevitably result in users surreptitiously writing down passwords, [which compromises security].

'658 Patent at 1:30–43.

The patent describes one prior-art product to make authentication easier. That product requires the user to possess a card that generates and displays an unpredictable, one-time access code that changes every minute. When logging in to the system, the user provides the code which can be verified by the system. *See id.* at 1:44–53.

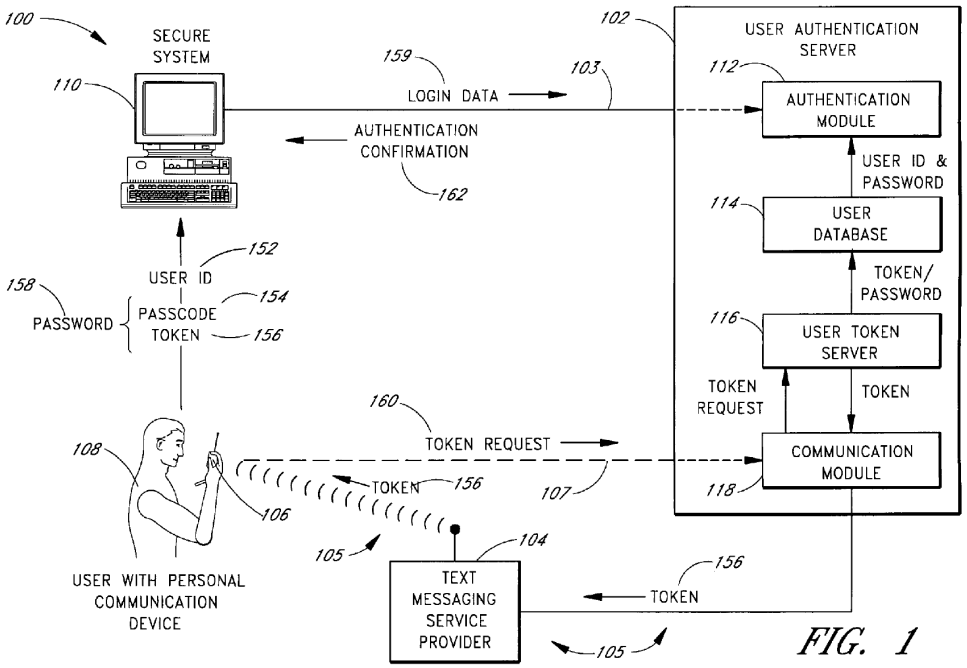

FIG. 1

The patent teaches a system with similar benefits without requiring the user to carry such a card. As shown in FIG. 1 (above), a token server (116) running on a user authentication server (102) generates a random token in response to a user request (160) for a new password. The server (102) creates the new password based on a secret passcode known to the user and the to-

ken, and then sets the user's password as the new password in a user database (114). A communication module (118) transmits the token (156) to the user's personal communication device (106), such as a mobile phone. The user forms the password from the secret passcode and received token and submits the password to access the secure system (100). *See generally* '658 Patent at [57], 4:2–51.

The patent includes two independent claims that collectively include four of the five disputed terms. Claim 1 is directed to:

> 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;
>
> **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.

'658 Patent at 11:43–57 (disputed terms bolded). Claim 5 is directed to a system that implements the method:

> 5. A user authentication system comprising:
>
> a computer processor;
>
> a user database configured to associate a user with a personal communication device possessed by the user, said personal communication device configured to communicate over a cell phone network with the user authentication system;
>
> a control module executed on the computer processor configured to create a new password based at least upon a token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user, the control module further configured to set a **password** associated with the user to be the new password;
>
> a communication module configured to transmit the token to the personal communication device through the cell phone network; and
>
> an authentication module configured to receive the **password** from the user through a secure computer network, said secure computer network being different from the cell phone network, wherein the user has an account on the secure computer network, wherein the authentication module **activates access to the account in response to the password** and deactivates the account within a predetermined amount of time after activating the account, such that said account is not accessible through any password via the secure computer network.

Id. at 12:20–47 (disputed terms bolded). For each of the disputed terms, Dynapass asks for a "plain and ordinary meaning" construction. Defendants, on the other hand, propose specific language.

II. GENERAL LEGAL STANDARDS

"[T]he claims of a patent define the invention to which the patentee is entitled the right to exclude." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc). As such, if the parties dispute the scope of the claims, the court must determine their meaning. *See, e.g.*, *Verizon Servs. Corp. v. Vonage Holdings Corp.*, 503 F.3d 1295, 1317 (Fed. Cir. 2007) (Gajarsa, J., concurring in part); *see also Markman v. Westview Instruments, Inc.*, 517 U.S. 370, 390 (1996), *aff'g*, 52 F.3d 967, 976 (Fed. Cir. 1995) (en banc).

Claim construction, however, "is not an obligatory exercise in redundancy." *U.S. Surgical Corp. v. Ethicon, Inc.*, 103 F.3d 1554, 1568 (Fed. Cir. 1997). Rather, "[c]laim construction is a matter of [resolving] disputed meanings and technical scope, to clarify and when necessary to explain what the patentee covered by the claims . . . ." *Id.* A court need not "repeat or restate every claim term in order to comply with the ruling that claim construction is for the court." *Id.*

When construing claims, "[t]here is a heavy presumption that claim terms are to be given their ordinary and customary meaning." *Aventis Pharm. Inc. v. Amino Chems. Ltd.*, 715 F.3d 1363, 1373 (Fed. Cir. 2013) (citing *Phillips*, 415 F.3d at 1312–13). Courts must therefore "look to the words of the claims themselves . . . to define the scope of the patented invention." *Id.* (citations omitted). The "ordinary and customary meaning of a claim term is the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention, i.e., as of the effective filing date of the patent application." *Phillips*, 415 F.3d at 1313. This "person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification." *Id.*

Intrinsic evidence is the primary resource for claim construction. *See Power-One, Inc. v.*

DOCKET ALARM

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.