Trials@uspto.gov
Tel: 571-272-7822

Paper 19
Entered: March 23, 2018

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS INC.,
Petitioner,

v.

TEXTILE COMPUTER SYSTEMS, INC.,
Patent Owner.

Case IPR2017-00296
Patent 8,505,079 B2

Before JUSTIN T. ARBES, STACEY G. WHITE, and SCOTT B. HOWARD, *Administrative Patent Judges*.

HOWARD, *Administrative Patent Judge*.

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

I. INTRODUCTION

Unified Patents Inc. ("Petitioner") filed a Petition (Paper 2, "Pet.") to institute an *inter partes* review of claims 1, 3, 6–9, 11, 13, and 16–19 of U.S. Patent No. 8,505,079 B2 (Ex. 1001, "the '079 patent") pursuant to 35 U.S.C. §§ 311–19. Textile Computer Systems, Inc. ("Patent Owner") filed a Patent Owner Preliminary Response. Paper 8 ("Prelim. Resp."). We instituted an *inter partes* review of claims 1, 3, 6–9, 11, 13, and 16–19 on certain grounds of unpatentability alleged in the Petition (Paper 9, "Dec.").

After institution of trial, Patent Owner filed a Patent Owner Response (Paper 13, "PO Resp."). Petitioner filed a Reply (Paper 17, "Reply"). Neither Patent Owner nor Petitioner requested an oral hearing. *See* Paper 18.

The Board has jurisdiction under 35 U.S.C. § 6(b). This Final Written Decision is entered pursuant to 35 U.S.C. § 318(a) as to the patentability of the claims for which we instituted trial. For the reasons that follow, we conclude that Petitioner has not demonstrated by a preponderance of the evidence that claims 1, 3, 6–9, 11, 13, and 16–19 of the '079 patent are unpatentable.

II. BACKGROUND

A. Related Proceedings

The parties identify the following former proceedings[1] involving the '079 patent: *Textile Comp. Sys., Inc. v. Fort Worth City Credit Union*, No. 2:16-cv-01048 (E.D. Tex.); *Textile Comp. Sys., Inc. v. Sabine Fed. Credit Union*, No. 2:16-cv-01047 (E.D. Tex.); and *Textile Comp. Sys., Inc. v.*

[1] We take notice that all of the cases have settled.

E. Tex. Prof'l Credit Union, No. 2:16-cv-00702 (E.D. Tex.). Pet. 73; Paper 4, 1.

B. The '079 Patent

The '079 patent "relates to security protocols for use in securing and/or restricting access to personal other confidential information, physical locations and the like." Ex. 1001, 1:6–8. According to the '079 patent, the protection of personal information "is of ever increasing concern" and has led to the use of "various security protocols employed for the protection of such resources," which "almost universally include[] some means for authenticating the identity of a person, entity, device or the like attempting to gain access to a secured resource." *Id.* at 1:16–28. However, "a security breach in connection with a single secured resource may jeopardize the security of all other secured resources." *Id.* at 1:42–44.

The '079 patent is directed to improving "the prior art by providing a system and related method by which authentication may be more securely conducted." *Id.* at 1:45–49. The '079 patent provides "a system and related method that is robust in specific implementation and readily usable" and "is economical in implementation and therefore readily accessible to virtually any application." *Id.* at 1:49–56.

The invention disclosed in the '079 patent is a transaction protocol between three parties—the end user (for example, a purchaser of an item), a service client (for example, a seller of goods or services), and a service provider (for example, a credit card processor)—that is conducted with six messaging steps. *See, e.g., id.* at Figs. 1, 4, 1:60–2:7, 2:27–38, 4:15–47, 7:14–8:3. Figure 4 of the '079 patent, as annotated by Petitioner (Pet. 3), is shown below:

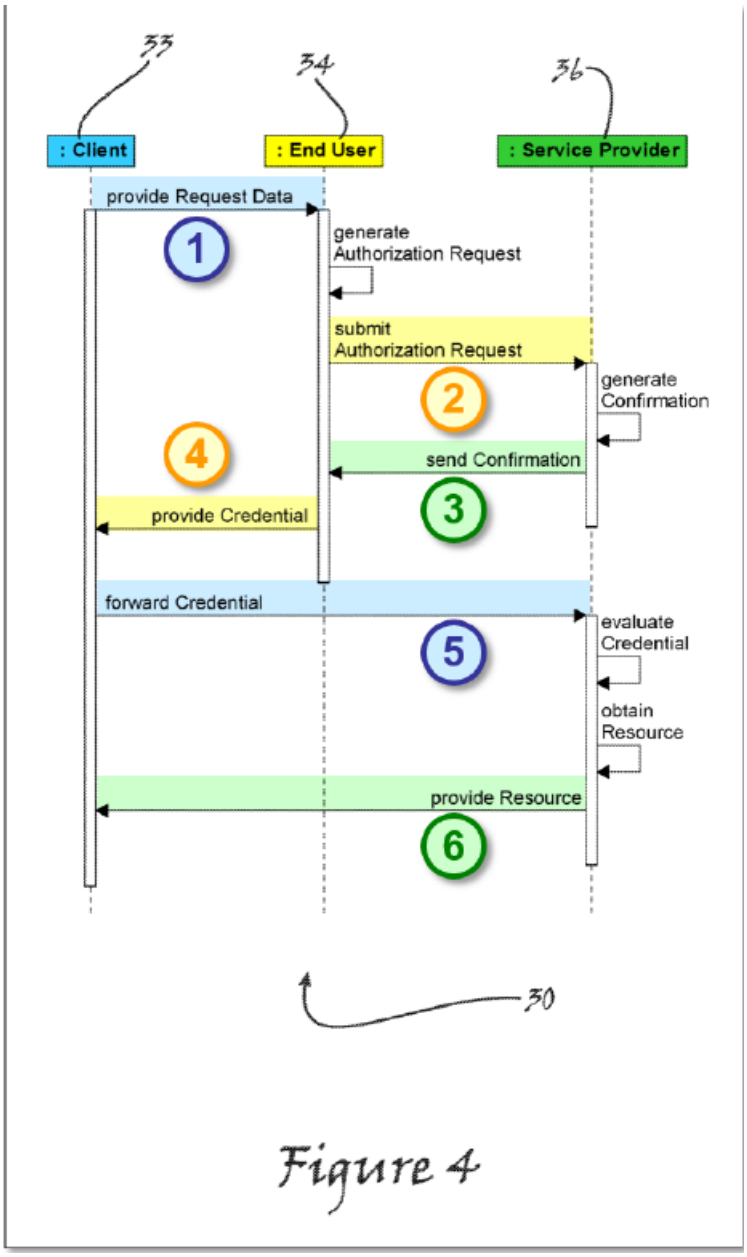

Figure 4

Figure 4 shows "various interactions [that] generally take place during the operation of the authentication system and method of the present invention" (Ex. 1001, 3:15–17) in which the six different messaging steps are color coded based on the sender—blue for the service client, yellow for the end user, and green for the service provider (*see* Pet. 2–4).

First, the service client sends data that will be used to generate a request to the end user. Ex. 1001, Fig. 4, 5:35–45. Second, the end user sends a request based on the received data to the service provider. *Id.* at Fig. 4, 5:45–49. Once the service provider receives the message, it "determines whether the end user 34 making the request is authorized or otherwise permitted to make use of the authentication system 30." *Id.* at 5:50–54; *see also id.* at 13:34–53. The system will continue only if the service provider authenticates the identity of the end user; otherwise, it will terminate. *Id.* at 5:54–60, 13:34–53. The '079 patent states that a critical aspect of the present invention is preventing the service client from having access to the common identifier of the secured resource that can be used to gain access to the secured resource without again gaining authorization from the end user:

> *In a critical aspect* of the authentication system 30 and method 46 *of the present invention*, an additional security measure is implemented by requiring that the service client 33 be restricted from access to the common identifier for the secured resource, e.g. the account number for a credit card or financial deposit account; the Social Security Number of a patient; the account number of an ATM card; or the like. . . .
>
> *In accordance with a critical aspect of the present invention*, however, the automobile fueling station, restaurant or on-line retailer cannot be provided with or otherwise be made aware of either the consumer's credit card or checking account number and also must not be given any information that would allow the automobile fueling station, restaurant or on-line retailer to repeat the transaction without again obtaining authorization from the consumer.

Id. at 8:4–10, 10:29–36 (emphases added); *see also id.* at 7:14–46 (emphasizing the importance of restricting the service client from having full access to the secured resource).

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.