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

SMART AUTHENTICATION IP, LLC Plaintiff, v. UNITED SERVICES AUTOMOBILE ASSOCIATION, Defendant.	Civil Action No. 2:16-cv-01232-JRG **JURY TRIAL DEMANDED** (LEAD CASE)
SMART AUTHENTICATION IP, LLC, Plaintiff, v. LOGMEIN, INC., Defendant.	Civil Action No. 2:16-cv-01234-JRG **JURY TRIAL DEMANDED** (CONSOLIDATED CASE)

FIRST AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Smart Authentication IP, LLC ("Smart Authentication"), by way of this First Amended Complaint against Defendant LogMeIn, Inc. ("LogMeIn") alleges as follows:

PARTIES

1. Plaintiff Smart Authentication is a limited liability company organized and existing under the laws of the State of Texas, having its principal place of business at 1400 Preston Road, Suite 400 Plano, TX 75093.

2. On information and belief, Defendant LogMeIn is a corporation organized and existing under the laws of the State of Delaware, with its principal place of business located at 320

Summer Street, Boston, MA 02210.

JURISDICTION AND VENUE

3. This is an action under the patent laws of the United States, 35 U.S.C. §§ 1, *et seq.*, for infringement by LogMeIn of claims of U.S. Patent No. 8,082,213 ("the '213 patent" or "Patent-in-Suit").

4. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

5. LogMeIn is subject to the personal jurisdiction of this Court because, *inter alia*, upon information and belief, (i) LogMeIn has done and continues to do business in the state of Texas, and (ii) LogMeIn has committed and continues to commit acts of patent infringement in the State of Texas, including by making, using, offering to sell, and/or selling accused products and services in Texas.

6. Venue is proper in this judicial district under 28 U.S.C. §§ 1391(b), 1391(c), and 1400(b) because, *inter alia*, on information and belief, (i) LogMeIn has done and continues to do business in this district; (ii) LogMeIn has committed and continues to commit acts of patent infringement in this district, including making, using, offering to sell, and/or selling accused products and services in this district, and/or importing accused products and services into this district, including by Internet sales; (iii) Plaintiff Smart Authentication is located in this district, and (iv) the Patent-in-Suit is assigned to Plaintiff.

BACKGROUND

7. On December 20, 2011, the United States Patent and Trademark Office duly and lawfully issued U.S. Patent No. 8,082,213. A true and correct copy of the '213 patent is attached as Exhibit A.

8. Jarlath Lyons invented the technology claimed in the Patent-in-Suit.

9. Smart Authentication is the assignee and owner of the right, title, and interest in and to the ’213 patent, including the right to assert all causes of action arising under said patent and the right to any remedies for infringement.

10. The inventions of the ’213 Patent generally relate to methods and systems for multi-factor authentication of users over multiple communications mediums.

11. The Patent-in-Suit discloses an Authentication Service Provider (“ASP”), which “is generally implemented above a software and hardware platform or platforms … that include operating systems, lower-level applications, and computer-server hardware.” Ex. A, col. 4:13-16. “In many embodiments, the ASP … is a software implemented service that runs on one or more computer systems interconnected by various communications media with both ASP clients and users.” Ex. A, col. 2:47-50. In certain embodiments, the “ASP may interact with the user via two different communications media, such as a combination of the Internet and a cell phone.” Ex. A, col. 3:23-25.

12. In another example of disclosed embodiments, “[t]he [] third interface 208 allows the ASP to interface with user devices through alternative communications media, such as a cell phone, fax machine, telephone, or other communications devices. The third interface 208 allows the ASP to interface with virtually any network enabled resource through an appropriate medium, including both physical devices such as a cell phone, fax machine, telephone, or other communications devices, and also soft devices, such as an instant messaging account, or an email account.” Ex. A, col. 3:37-46.

13. As one example of an asserted claim, the ’213 Patent recites a novel method of authenticating a user of an authentication service where an authentication-service client communicates with the user through a first communication medium. The authentication service

receives user-identifying information from the authentication-service client, and uses the received user-identifying information to carry out an authentication procedure to authenticate the user by sending information to the user through a communications medium different from the first communications medium. The authentication result is then returned to the authentication service client.

14. In another example of an asserted claim, the ’213 Patent recites the novel method described above, wherein the user authentication service further uses electronically-encoded information about the user to retrieve all stored user authentication policies for the user, and conducting the user authentication procedure as permitted by the stored policies. The authentication result is then returned to the authentication service client.

15. LogMeIn offers the “Pro” and “Central” products for access and management of computers remotely for individuals, small businesses, and IT Professionals. LogMeIn offers the “Rescue” product for the on-demand remote access for IT professionals, Help Desk, and Technicians. LogMeIn also offers the “LastPass” product for managing passwords.

16. LogMeIn’s products use two-factor authentication over multiple communications mediums by first requiring the user to enter a LogMeIn ID and password through the Internet via a browser or mobile app, and then by requiring the user to verify his or her identity by entering a one-time code received by means of a text message, an e-mail message, an authenticator app on the user’s mobile device, or other means.

17. During the two-factor authentication process, LogMeIn also uses the electronically-encoded information about the user to retrieve all authentication-related policies for that user. For example, the user may set up a primary and back-up methods of receiving the one-time verification code. Once the authentication-related policies are retrieved, LogMeIn conducts the

authentication procedure and returns the authentication results.

COUNT I: INFRINGEMENT OF U.S. PATENT NO. 8,082,213

18. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

19. Upon information and belief, LogMeIn has infringed, and continues to infringe at least claims 1, 2, 3, 4, 5, 7, 8, 9, 10, 12, 13, 14, 15, and 16 of the ’213 patent pursuant to 35 U.S.C. § 271(a) by making, using, offering to sell, and/or selling in the United States products and/or services, including, but not limited to “Pro,” “Central,” “Rescue,” and “LastPass”, and also including LogMeIn products for which users are able to log in via (i) LogMeIn.com; (ii) LogMeIn host software for Windows, 4.1.4141 and above; (iii) LogMeIn host software for Mac, 4.1.4132 and above; (iv) LogMeIn for iOS app, all versions; (v) LogMeIn for Android app, all versions except "Ignition" branded versions; (vi) join.me (all components), all versions; (vii) Cubby (apps and website), all versions; (viii) AppGuru.com; and (ix) meldium.com. *See* Exhibit B, “LogMeIn Central User Guide,” available at secure.logmein.com/welcome/webhelp/EN/CentralUserGuide/LogMeIn/c_common_Security_TwoStep.html.

20. Upon information and belief, LogMeIn’s products and services infringe claim 1 by, for example, using, making, selling, and/or offering for sale, a user authentication service comprising one or more computer systems, stored user-authentication policies specified by the user, account interface routines by which the user specifies, modifies, adds, and deletes user-authentication policies, and authentication-interface routines that implement an authentication interface. In LogMeIn’s user-authentication service, the user initiates a transaction with the authentication-service client (such as LogMeIn’s website and/or other products, services, versions, or components identified in ¶19) (Ex. B), and the authentication-service client submits an authentication request to LogMeIn’s authentication-service through a first communications

medium (such as the Internet via a browser) (Ex. B) or through a second communications medium (such as a mobile application running on a tablet or on a computer) (Ex. B). In LogMeIn's user-authentication service, when specified by stored user-authentication policies, the authentication-interface routines employ a variable-factor authentication, such as providing secret information (such as a password or one-time code generated by LogMeIn's authentication service) and demonstrating control of a tangible object (such as a user's phone) (Exs. B). During LogMeIn's authentication process, the user communicates with the user-authentication service through a third communications medium (such as receiving a security code via an SMS text message or email) and a user device different from that employed by the user to initiate the transaction with the authentication-service client (such as a mobile phone) (Exs. B).

21. In another example, LogMeIn's products and services infringe claim 2, in which the user-authentication service of claim 1 stores user-authentication policies and user information for multiple users. *See, e.g.*, accused products which provide authentication of multiple users. Ex. B.

22. In another example, LogMeIn's products and services infringe claim 3, in which the user-authentication service of claim 1 retrieves all stored user-authentication policies for the user, which include alternative authentication methods. *See* Ex. B. In accordance with the retrieved policies, LogMeIn's user authentication service conducts the alternative authentication procedure, and returns the authentication result to the authentication service client.

23. In another example, LogMeIn's products and services further infringe claim 4, in which the authentication policy may comprise a uni-directional or bi-directional exchange of information with the user through the third communications medium (such as receiving a security code via an SMS text message or email) (Ex. B).

24. In another example, LogMeIn's products and services infringe claim 5, in which the information of claim 4 is a password (such as LogMeIn's security code) that the user can subsequently input to the authentication-service client (such as LogMeIn's website) to prove to the authentication-service client that the user has been authenticated by the user-authentication service.

25. In another example, LogMeIn's products and services infringe claim 7, wherein the stored user information includes one or more of user's name, the user's address, the user's billing information, a password specified by the user, and the user's contact information.

26. In another example, LogMeIn's products and services infringe claim 8, wherein the user's contact information includes one or more of user's landline and cell phones, contact information for the user's trusted hand-held computing devices, and an email address.

27. In another example, LogMeIn's products and services infringe claim 9, wherein a user-authentication policies that specify constraints and parameters for mobile phone and email authentication, such as the presence or absence of mobile phone numbers, an authentication email address, and an authenticator app. Additionally, for example, LogMeIn's user authentication system includes constraints and parameters in which two-factor authentication is bypassed for trusted devices.

28. In another example, LogMeIn's products and services infringe claim 10, wherein constraints include a communications-medium-related constraint, such as the absence or presence of an email address to be used for backup authentication is a communications-medium-related constraint. Additionally, for example, the bypassing of two-factor authentication for trusted devices is a user authentication action, or, alternatively, an event constraint.

29. Upon information and belief, LogMeIn's products and services infringe claim 12 by, for

example, performing "Two-Step Verification." *See* Ex. B. In one example, LogMeIn's user authentication client (such as LogMeIn's website and/or other products, services, versions, or components identified in ¶19, including, for example, the accounts.logme.in website), communicates with the user via an application (mobile or desktop) or the Internet via a browser. *See* Ex. B. LogMeIn's user authentication service receives user-identifying information, such as the user's LogMeIn ID. LogMeIn's user authentication service then uses the user-identifying information to carry out an authentication procedure by sending to the user an authentication code via a text message or backup email, which is a communication medium that is different from the first communications medium (such as an application (mobile or desktop) or the Internet via a browser). *See* Ex. B. LogMeIn's user authentication service then returns an authentication result to the user authentication client.

30. In another example, LogMeIn's products and services infringe claim 13, by, for example, performing the method of claim 13, wherein, as part of the authentication procedure, the authentication service transmits information (such as a security code) to the user of the authentication service which the user of the authentication service then subsequently transmits to the authentication-service client (such as LogMeIn's website).

31. In another example, LogMeIn's products and services infringe claim 14 by, for example, performing the method of claim 12, and further retrieving all stored user-authentication policies for the user, which includes the backup authentication methods. *See* Ex. B. In accordance with the retrieved backup policies, LogMeIn's user authentication service conducts the backup authentication procedure, and returns the authentication result to the authentication service client.

32. In another example, LogMeIn's products and services infringe claim 15, in which the authentication policy may comprise a uni-directional or bi-directional exchange of information

with the user through the third communications medium (such as receiving a security code via an SMS text message or email).

33. In another example, LogMeIn's products and services infringe claim 16, in which the information of claim 15 is a password (such as LogMeIn's security code) that the user can subsequently input to the authentication-service client (such as LogMeIn's website) to prove to the authentication-service client that the user has been authenticated by the user-authentication service.

34. Upon information and belief, LogMeIn has committed and continues to commit the foregoing infringing activities without a license.

35. LogMeIn has infringed and continues to infringe despite an objectively high likelihood that its actions constitute infringement of Smart Authentication's valid patent rights. On information and belief, LogMeIn knew of or should have known of this objectively high risk at least as early as when it became aware of the '213 patent and claims asserted by Smart Authentication in Smart Authentication's original complaint in this action dated November 4, 2016, and further after being served with Smart Authentication's Infringement Contentions pursuant to Local Patent Rule 3-1 on January 17, 2017. Thus, LogMeIn's infringement of the Patent-in-Suit has been and continues to be willful.

36. Smart Authentication seeks a willfulness finding against LogMeIn based on the above and on other and additional grounds, and treble damages under 35 U.S.C. § 284.

37. Smart Authentication has been and will continue to be irreparably harmed and damaged by LogMeIn's infringement of the '213 patent and has no adequate remedy at law. Smart Authentication has no adequate remedy at law and is entitled to an injunction against Defendant's continuing infringement of the '213 patent.

38. The acts of infringement by LogMeIn will continue unless enjoined by this Court.

PRAYER FOR RELIEF

WHEREFORE, Smart Authentication prays for the judgment in its favor against LogMeIn, and specifically, for the following relief:

A. Entry of judgment in favor of Smart Authentication against LogMeIn on all counts;

B. Entry of judgment that LogMeIn has infringed the Patent-in-Suit;

C. Entry of judgment that LogMeIn's infringement of the Patent-in-Suit has been willful.

D. An order permanently enjoining LogMeIn from infringing the Patent-in-Suit;

E. Award of compensatory damages adequate to compensate Smart Authentication for LogMeIn's infringement of the Patent-in-Suit, in no event less than a reasonable royalty trebled as provided by 35 U.S.C. § 284;

F. Smart Authentication's costs;

G. Pre-judgment and post-judgment interest on Smart Authentication's award; and

H. All such other and further relief as the Court deems just or equitable.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38 of the Fed. R. Civ. Proc., Plaintiff hereby demands trial by jury in this action of all claims so triable.

Dated: January 23, 2017

Respectfully submitted,

/s/ Dmitry Kheyfits

Dmitry Kheyfits — Lead Counsel
New York State Bar No. 4743795
dkheyfits@kheyfits.com

Andrey Belenky
New York State Bar No. 4524898
abelenky@kheyfits.com
KHEYFITS P.C.
1140 Avenue of the Americas
9th Floor
New York, New York 10036
Tel. (212) 203-5399
Fax. (212) 203-6445

/s/ L. Charles van Cleef

L. Charles van Cleef TX SB #00786305
Van Cleef Law Office
PO Box 2432
Longview, TX 75606-2432
Telephone: (903) 248-8244
Facsimile: (903) 248-8249
charles@vancleef.pro

Attorneys for Plaintiff Smart Authentication IP, LLC

CERTIFICATE OF SERVICE

The undersigned hereby certifies that all counsel of record who are deemed to have consented to electronic service are being served with a copy of this document via the Court's CM/ECF system per Local Rule CV-5 this Monday, January 23, 2017.

/s/ L. Charles van Cleef
L. Charles van Cleef