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

SMART AUTHENTICATION IP, LLC, Plaintiff, v. DISCOVER FINANCIAL SERVICES, DFS SERVICES LLC, AND DISCOVER BANK, Defendants.	Civil Action No. 2:17-cv-279 **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Smart Authentication IP, LLC ("Smart Authentication"), by way of this Complaint against Defendants Discover Financial Services ("DFS"), DFS Services LLC ("DFSLLC"), and Discover Bank ("DB") (DFS, DFSLLC, and DB are collectively referred to as "Discover" or "Defendants" herein) 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 DFS is a corporation organized and existing under the laws of the State of Delaware, with a principal office located at 2500 Lake Cook Road, Riverwoods, Illinois 60015, and it conducts business in this judicial district.

3. On information and belief, Defendant DFSLLC is a limited liability company organized and existing under the laws of the State of Delaware, with a principal office located at 2500 Lake Cook Road, Riverwoods, Illinois 60015, and it conducts business in this judicial district. On

information and belief, DFSLLC is a wholly owned subsidiary of DFS.

4. On information and belief, DB is a banking corporation organized under the laws of the State of Delaware, with a principal place of business located at 502 E. Market Street, Greenwood, DE 19950, and it conducts business in this judicial district. On information and belief, DB is a wholly owned subsidiary of DFS.

JURISDICTION AND VENUE

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

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

7. Defendants are subject to the personal jurisdiction of this Court because, *inter alia*, upon information and belief, (i) Defendants have done and continue to do business in the State of Texas, (ii) DFSLLC is registered to transact business in the State of Texas, (iii) DB has registered for a State of Texas Taxpayers ID#, (iv) DFSLLC and DB are wholly owned subsidiaries of DFS, and (iii) Defendants have committed and continue 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.

8. 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) Defendants have done and continue to do business in this district; (ii) Defendants have committed and continue 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

9. 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.

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

11. 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.

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

13. 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.

14. 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.

15. 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.

16. 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.

17. Defendants offer banking, insurance, investing, and e-commerce products and services to customers. Defendants' products and services are accessible to users via Defendants' website at www.discover.com, and Defendants' iOS and Android apps.

18. Defendants' products and services use two-factor authentication over multiple communications mediums by first requiring the user to enter a Discover "User ID" and password over 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 phone call, text message, or an e-

mail message.

19. During the two-factor authentication process, Defendants also use the electronically-encoded information about the user to retrieve all authentication-related policies for that user. For example, the user may set up several methods of receiving the one-time verification code. Once the authentication-related policies are retrieved, Defendants conduct the authentication procedure and return the authentication results.

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

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

21. Upon information and belief, Defendants have infringed, and continue to infringe at least claims 1, 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, their banking, insurance, investing, and e-commerce products and services to customers, including Defendants’ products and services accessible to users via the Defendants’ website at www.discover.com (Ex. B and C), and Defendants’ mobile apps (Ex. B-E).

22. Upon information and belief, Defendants’ 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 Defendants’ user-authentication service, the user initiates a transaction with the authentication-service client (such as Defendants’ website) (Ex. B and C), and the authentication-service client submits an authentication request to Defendants’ authentication-service through a first communications medium (such as the Internet via a browser) (Ex. B and

C) or through a second communications medium (such as a mobile application running on a tablet or on a computer) (Ex. B-E). In Defendants' 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 Defendants' authentication service) and demonstrating control of a tangible object (such as a user's phone) (Exs. B and C). During Defendants' authentication process, the user communicates with the user-authentication service through a third communications medium (such as receiving a code via a phone call, 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 and C).

23. In another example, Defendants' 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* Exs. B and C. In accordance with the retrieved policies, Defendants' user authentication service conducts the alternative authentication procedure, and returns the authentication result to the authentication service client.

24. In another example, Defendants' 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 code via a phone call, SMS text message, or email) (Ex. B and C).

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

service.

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

27. In another example, Defendants' products and services infringe claim 8, wherein the user's contact information includes one or more of the user's landline and cell phones, and an email address.

28. In another example, Defendants' products and services infringe claim 9, wherein a user-authentication policy specifies constraints and parameters for mobile phone and email authentication, such as the presence or absence of mobile phone numbers and an authentication email address.

29. In another example, Defendants' 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.

30. Upon information and belief, Defendants' products and services infringe claim 12 by, for example, performing "Enhanced Account Verification." *See* Exs. B and C. In one example, Defendants' user authentication client, such as the discover.com website, communicates with the user via a mobile application or the Internet via a browser. *See* Exs. B and C. Defendants' user authentication service receives user-identifying information, such as the user's "User ID." Defendants' user authentication service then uses the user-identifying information to carry out an authentication procedure by sending to the user a code via a text message, which is a communication medium that is different from the mobile application or the Internet via a browser. *See* Exs. B and C. Defendants' user authentication service then returns an

authentication result to the user authentication client.

31. In another example, Defendants' 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 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 Defendants' website).

32. In another example, Defendants' 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 alternative authentication methods. *See* Exs. B and C. In accordance with the retrieved policies, Defendants' user authentication service conducts the alternative authentication procedure, and returns the authentication result to the authentication service client.

33. In another example, Defendants' 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 code via a phone call, SMS text message, or email).

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

35. Smart Authentication has been and will continue to be irreparably harmed and damaged by Defendants' 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 Defendants' continuing infringement of the '213 patent.

36. The acts of infringement by Defendants will continue unless enjoined by this Court.

PRAYER FOR RELIEF

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

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

B. Entry of judgment that Defendants have infringed the Patent-in-Suit;

C. An order permanently enjoining Defendants from infringing the Patent-in-Suit;

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

E. Smart Authentication's costs;

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

G. 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: April 7, 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