IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

KARETEK HOLDINGS LLC, Plaintiff, v. **STRIPE, INC.,** Defendant.	Civil Action No.: **TRIAL BY JURY DEMANDED**

COMPLAINT FOR INFRINGEMENT OF PATENT

Now comes, Plaintiff, Karetek Holdings LLC ("Plaintiff"), by and through undersigned counsel, and respectfully alleges, states, and prays as follows:

NATURE OF THE ACTION

1. This is an action for patent infringement under the Patent Laws of the United States, Title 35 United States Code ("U.S.C.") to prevent and enjoin Defendant Stripe, Inc. (hereinafter "Defendant"), from infringing and profiting, in an illegal and unauthorized manner, and without authorization and/or consent from Plaintiff from U.S. Patent No 7,373,515 ("the '515 Patent" or the "Patent-in-Suit"), which is attached hereto as Exhibit 1 and incorporated herein by reference, and pursuant to 35 U.S.C. §271, and to recover damages, attorney's fees, and costs.

THE PARTIES

2. Plaintiff is a Texas limited liability company with its principal place of business at 15922 Eldorado Parkway – Suite 500-1711, Frisco, Texas 75035.

3. Upon information and belief, Defendant is a corporation organized under the laws of Delaware, having a principal place of business at 510 Townsend Street, San Francisco, CA 94107. Upon information and belief, Defendant may be served with process c/o The Corporation Trust Company Corporation Trust Center 1209 Orange St, Wilmington, New Castle, DE, 19801.

JURISDICTION AND VENUE

4. This is an action for patent infringement in violation of the Patent Act of the United States, 35 U.S.C. §§1 *et seq*.

5. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§1331 and 1338(a).

6. This Court has personal jurisdiction over Defendant by virtue of its systematic and continuous contacts with this jurisdiction and its residence in this District, as well as because of the injury to Plaintiff, and the cause of action Plaintiff has risen in this District, as alleged herein.

7. Defendant is subject to this Court's specific and general personal jurisdiction pursuant to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in this forum state and in this judicial.

8. Venue is proper in this judicial district pursuant to 28 U.S.C. §1400(b) because Defendant resides in this District under the Supreme Court's opinion in *TC Heartland v. Kraft Foods Group Brands LLC,* 137 S. Ct. 1514 (2017) through its incorporation in this District.

FACTUAL ALLEGATIONS

9. On May 13, 2008, the United States Patent and Trademark Office ("USPTO") duly and legally issued the '515 Patent, entitled "MULTI-FACTOR AUTHENTICATION SYSTEM" after a full and fair examination. The '515 Patent is attached hereto as Exhibit 1 and incorporated herein as if fully rewritten.

10. Plaintiff is presently the owner of the '515 Patent, having received all right, title and interest in and to the '515 Patent from the previous assignee of record. Plaintiff possesses all

rights of recovery under the '515 Patent, including the exclusive right to recover for past infringement.

11. To the extent required, Plaintiff has complied with all marking requirements under 35 U.S.C. § 287.

12. The invention claimed in the '515 Patent comprises a multi-factor authentication system and method.

13. Claim 20 of the '515 Patent recites a method for gaining access by a user to a network resource.

14. Claim 20 of the '515 Patent states:

> "20. A method of granting access to a suspect user seeking to access a network resource, comprising the steps of:
>
> (a) first,
>
> (i) maintaining credentials of the authorized user such that the credentials are retrievable based on the user ID,
>
> (ii) receiving a user ID, registration code, and suspect credentials,
>
> (iii) comparing the suspect credentials with the credentials maintained in association with the user ID, and
>
> (iv) upon a successful authentication of the user ID by matching the suspect credentials with the maintained credentials, communicating the user ID and registration code to an authentication authority; and
>
> (b) thereafter, granting access to the network resource to a suspect user upon,
>
> (i) receiving a user ID and passcode from the suspect user,
>
> (ii) communicating the user ID and passcode to the authentication authority, and
>
> (iii) receiving an indication of a successful passcode comparison by the authentication authority." See Exhibit 1.

15. The '515 Patent identified computer-centric or internet-centric technological problems that needed to be solved. See generally Ex. 1 at Background, Col.1-2.

16. More particularly, the '515 Patent identified that a user ID and password are often required in order for a suspect user to gain access to a network resource from an access authority

of a computer network. Ex. 1. at Col. 1:24-29. The access authority may comprise a server of the computer network, which grants access once the user ID has been authenticated using the password received from the suspect user. Ex. 1 at Col. 1:29-32. The access authority may include security privileges for granting specific types of access by authenticated users, and the access authority may additionally perform the authentication of suspect users. Ex. 1 at Col. 1:32-36.

17. The '515 Patent identified that in order to reduce confusion, "users typically choose easy-to-remember-passwords. Otherwise, users tend to forget complex passwords and record the passwords in easily accessible areas for later reference. For example, many users maintain a list of user IDs and passwords in a spreadsheet or text file on their computer or personal digital assistant. Programs even have been written to help maintain user ID and password combinations." Ex. 1 at Col. 1:39-47.

18. The '515 Patent identified that computer-centric problems or internet-centric problems existed as a result of the easy to remember passwords chosen by user.

19. Namely, "Enterprises, such as corporations, Internet service providers, portals, application service providers (ASPs), e-commerce providers, online financial services, etc., must manage user IDs and passwords for their users. Allowing users to employ simple passwords reduces security at a time when security attacks are increasing and are increasingly expensive when they occur. On the other hand, enforcing the use of complex passwords and requiring passwords to be changed frequently increases security, but also increases cost in the form of help desk and customer service calls for the resetting of passwords. The systems that have been developed to allow users to use personal information to reset a password automatically without human intervention tend to be less secure because personal information can be guessed or obtained surreptitiously. Some systems, for example, use information from credit reports—despite the fact

that credit bureaus are in the business of proactively selling that information." Ex. 1. at Col. 1:47-65.

20. There were prior attempts to overcome these problems.

21. Namely, the prior art provided single sign-on systems "in which a user is able to authenticate to a single trusted authentication server, which then propagates that authentication to multiple access authorities. While the use of a single authentication server eases the user burden of remembering multiple passwords for accessing various network resources, such a system typically is limited to accessing network resources of a single enterprise. Such a system also is susceptible to a security problem known as "keys to the kingdom." If an attack gains access to the user ID and password required to authenticate to the authentication server, then access to all network resources relying upon that authentication server are compromised." Ex. 1 at Col. 1:67-Col. 2:11.

22. Additionally, in the prior arte there were stronger forms of authenticating user IDs. Namely, "hardware token such as USB tokens and time-based tokens—RSA's SecureID is an example—are now being utilized in some multi-factor authentication systems wherein these tokens are able to uniquely identify themselves. For example, a token utilizing physical access to a device and knowledge of a shared secret, such as a PIN, can construct a rotating key that matches a synchronized server key. Such a system is a "two-factor" authentication system because it requires something the user has, i.e., the token, in addition to something the user knows, i.e., the password. Unfortunately, each token in one of these two-factor authentication system is expensive, subject to loss, and typically restricted to use with one or more network resources of a particular computer network." Ex. 1 at Col. 2:12-28.

23. Claim 20 of the '515 Patent addressed the need for an improved multi-factor authentication system that overcomes one or more of the aforementioned computer-centric or internet-centric disadvantages of prior art authentication systems.

24. Specifically, to deal with each token in these two-factor authentication system being expensive, subject to loss, and typically restricted to use with one or more network resources of a particular computer network, the method of Claim 20 in the '515 patent requires (a) communicating a PIN and a first primary identification over *an ancillary communications network* to *an authentication authority*; (b) receiving an encrypted passcode over the ancillary communications network from the authentication authority; (c) decrypting the passcode *using a key of an asymmetric key pair*; and (d) communicating the *passcode and a user ID* over *a communications* network to *an access authority*. These specific elements (i.e., the ancillary communication network, the authentication authority, the use of a key of an asymmetric key pair, the passcode and a user ID, a communication network, and an access authority), as combined, accomplish the desired result decreasing cost, reducing the likelihood of, and may not be restricted to use with one or more network resources of a particular computer network. Further, these specific elements also accomplish these desired results to overcome the then existing problems in the relevant field of network communication systems. *Ancora Technologies, Inc. v. HTC America, Inc.*, 908 F.3d 1343, 1348 (Fed. Cir. 2018) (holding that improving computer security can be a non-abstract computer-functionality improvement if done by a specific technique that departs from earlier approaches to solve a specific computer problem). See also *Data Engine Techs. LLC v. Google LLC*, 906 F.3d 999 (Fed. Cir. 2018); *Core Wireless Licensing v. LG Elecs., Inc.*, 880 F.3d 1356 (Fed. Cir. 2018); *Finjan, Inc. v. Blue Coat Sys., Inc.*, 879 F.3d 1299 (Fed. Cir. 2018); *Uniloc USA, Inc. v. LG Electronics USA, Inc.*, 957 F.3d 1303 (Fed. Cir. April 30, 2020).

25. Claims need not articulate the advantages of the claimed combinations to be eligible. *Uniloc USA, Inc. v. LG Elecs. USA, Inc.*, 957 F.3d 1303, 1309 (Fed. Cir. 2020).

26. These specific elements of Claim 20 of the '515 Patent (i.e., the ancillary communication network, the authentication authority, the use of a key of an asymmetric key pair, the passcode and a user ID, a communication network, and an access authority) were an unconventional arrangement of elements because the prior art methodologies would simply use tokens to identify themselves by a rotating key that that matches a synchronized server key. By adding the specific elements (i.e., the ancillary communication network, the authentication authority, the use of a key of an asymmetric key pair, the passcode and a user ID, a communication network, and an access authority), Claim 20 of the '515 Patent was able to unconventionally generate a method for gaining access by a user to a network resource. *Cellspin Soft, Inc. v. FitBit, Inc.*, 927 F.3d 1306 (Fed. Cir. 2019)

27. Further, regarding the specific non-conventional and non-generic arrangements of known, conventional pieces to overcome an existing problem, the method of Claim 20 in the '515 Patent provides a method of gaining access to network that would not preempt all ways of confidentially authenticating a user because the data-rate control signal is based on the ancillary communication network, the authentication authority, the use of a key of an asymmetric key pair, the passcode and a user ID, a communication network, and an access authority, any of which could be removed or performed differently to permit a method of gaining access to network in a different way. *Bascom Global Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341 (Fed. Cir. 2016); See also *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245 (Fed. Cir. 2014).

28. Based on the allegations, it must be accepted as true at this stage, that Claim 20 of the '515 Patent recites a specific, plausibly inventive way of gaining access to a network and using

specific protocols rather than the general idea of confidentially authenticating a user. *Cellspin Soft, Inc. v. Fitbit, Inc.*, 927 F.3d 1306, 1319 (Fed. Cir. 2019), *cert. denied sub nom. Garmin USA, Inc. v. Cellspin Soft, Inc.*, 140 S. Ct. 907, 205 L. Ed. 2d 459 (2020).

29. Alternatively, there is at least a question of fact that must survive the pleading stage as to whether these specific elements of Claim 20 of the '515 Patent (i.e., the ancillary communication network, the authentication authority, the use of a key of an asymmetric key pair, the passcode and a user ID, a communication network, and an access authority) were an unconventional arrangement of elements. *Aatrix Software, Inc. v. Green Shades Software, Inc.*, 882 F.3d 1121 (Fed. Cir. 2018) See also *Berkheimer v. HP Inc.*, 881 F.3d 1360 (Fed. Cir. 2018), *cert. denied*, 140 S. Ct. 911, 205 L. Ed. 2d 454 (2020).

30. Defendant commercializes, inter alia, methods that perform all the steps recited in at least one claim of the '515 Patent. More particularly, Defendant commercializes, inter alia, methods that perform all the steps recited in Claim 20 of the '515 Patent. Specifically, Defendant makes, uses, sells, offers for sale, or imports a method that encompasses that which is covered by Claim 20 of the '515 Patent.

COUNT 1: Infringement of the '515 Patent

31. Plaintiff incorporates the above paragraphs herein by reference.

32. **Direct Infringement**. Defendant has been and continues to directly infringe one or more claims of the '515 Patent in at least this District by making, using, offering to sell, selling and/or importing, without limitation, at least the Defendant products identified in the charts incorporated into this Count below (among the "Exemplary Defendant Products") that infringe at least claim 20 of the '515 Patent also identified in the charts incorporated into this Count below

(the "Exemplary '515 Patent Claims") literally or by the doctrine of equivalents. On information and belief, numerous other devices that infringe the claims of the '515 Patent have been made, used, sold, imported, and offered for sale by Defendant and/or its customers.

33. Defendant also has and continues to directly infringe, literally or under the doctrine of equivalents, the Exemplary '515 Patent Claims, by having its employees internally test and use these Exemplary Products.

34. Exhibit 2 includes charts comparing the Exemplary '515 Patent Claims to the Exemplary Defendant Products. As set forth in these charts, the Exemplary Defendant Products practice the technology claimed by the '515 Patent. Accordingly, the Exemplary Defendant Products incorporated in these charts satisfy all elements of the Exemplary '515 Patent Claims.

35. Plaintiff therefore incorporates by reference in its allegations herein the claim charts of Exhibit 2.

36. Plaintiff is entitled to recover damages adequate to compensate for Defendants infringement.

DEMAND FOR JURY TRIAL

37. Plaintiff demands a trial by jury of any and all causes of action.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for the following relief:

a. That Defendant be adjudged to have directly infringed the '515 Patent either literally or under the doctrine of equivalents;

b. An accounting of all infringing sales and damages including, but not limited to, those sales and damages not presented at trial;

c. An award of damages pursuant to 35 U.S.C. §284 sufficient to compensate Plaintiff for the Defendant's past infringement and any continuing or future infringement up until the date that Defendant is finally and permanently enjoined from further infringement, including compensatory damages;

d. An assessment of pre-judgment and post-judgment interest and costs against Defendant, together with an award of such interest and costs, in accordance with 35 U.S.C. §284;

e. That Defendant be directed to pay enhanced damages, including Plaintiff's attorneys' fees incurred in connection with this lawsuit pursuant to 35 U.S.C. §285; and

f. That Plaintiff be granted such other and further relief as this Court may deem just and proper.

Dated: April 30, 2021

Respectfully submitted,

GAWTHROP GREENWOOD, PC

/s/ David W. deBruin

David W. deBruin, Esq. (#4846)
3711 Kennett Pike, Suite 100
Wilmington, DE 19807
Tel: (302) 777-5353
ddebruin@gawthrop.com

Counsel for Plaintiff
Karetek Holdings LLC