UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

EasyWeb Innovations, LLC *Plaintiff*, v. Socketlabs Acquisition LLC d/b/a Socketlabs *Defendant*.	Civil Action No. 24-CV-10698 **JURY TRIAL REQUESTED**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff EasyWeb Innovations, LLC ("EasyWeb" or "Plaintiff"), through its undersigned counsel, hereby alleges the following against Defendant Socketlabs Acquisition LLC ("Socketlabs" or "Defendant"):

NATURE OF THE ACTION

1. This is a civil action for patent infringement arising under the Patent Laws of the United States, 35 U.S.C. § 1 et seq.

THE PARTIES

2. Plaintiff EasyWeb Innovations, LLC is a New York limited liability company having a principal place of business at 3280 Sunrise Highway, Suite 171, Wantagh, New York 11793.

3. Defendant Socketlabs Acquisition LLC is a corporation organized and existing under the laws of Pennsylvania that maintains an established place of business at 676 E. Swedesford Rd., Suite 350B, Wayne, PA 19087 USA. On information and belief, Socketlabs also maintains physical office space in New Jersey, where its Director of Engineering sits.

JURISDICTION AND VENUE

4. This Court has exclusive subject matter jurisdiction over this case pursuant to 28 U.S.C. §§ 1331 and 1338(a) on the grounds that this action arises under the Patent Laws of the United States, 35 U.S.C. § 1 et seq., including, without limitation, 35 U.S.C. §§ 271, 281, 284, and 285.

5. This Court has personal jurisdiction over Defendant because it has engaged in systematic and continuous business activities in this District. As described below, Defendant has committed acts of patent infringement giving rise to this action within this District. Further, Defendant has, directly or through subsidiaries or intermediaries, committed acts of patent infringement in the State of New Jersey in this Judicial District as alleged in this Complaint.

6. Venue is proper in this District under 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to the claim occurred here. In addition, Defendant has committed acts of patent infringement in this District, and Plaintiff has suffered harm in this district.

7. Upon information and belief, Defendant manages the marketing, sales, and/or provision of services of its products to customers and/or potential customers located in New Jersey.

8. Defendant's Director of Engineering, David Schrenker, is a resident of New Jersey and, upon information and belief, maintains an office in New Jersey.

9. On information and belief, Defendant has sponsored an H1B employee with the job title of Software Engineer Back End, located in North Brunswick, New Jersey. The LCA Case number is I-200-24138-01014-7. See https://h1bgrader.com/h1b-sponsors/socketlabs-acquisition-llc-30q41xzgkq/lca/2024.

10.

PATENT-IN-SUIT

2. On October 30, 2018, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 10,114,905 (the "905 Patent"), entitled "Individual User Selectable Multi-Level Authorization Method for Accessing a Computer System." A true and correct copy of the 905 Patent is attached hereto as **Exhibit A**.

3. Plaintiff is the sole and exclusive owner of all right, title, and interest to and in, or is the exclusive licensee with the right to sue for, the 905 Patent (the "Patent-in-Suit") and holds the exclusive right to take all actions necessary to enforce its rights to the Patent-in-Suit, including the filing of this patent infringement lawsuit.

4. Plaintiff also has the right to recover all damages for infringement of the Patent-in-Suit as appropriate under the law.

5. The technologies of the Patent-in-Suit were invented by John D. Codignotto of Wantagh, New York. The 905 Patent generally covers user-customizable computer access security.

6. The 905 Patent is a continuation of the latest of a series of patent continuations, application No. 15/145,461, filed on May 3, 2016. The 905 Patent claims priority to Provisional application No. 60/123,821, filed on March 11, 1999.

7. Related patents (*i.e.*, family members) of the 905 Patent have been cited about 300 times, by some of the largest and most notable tech companies in the world, including Google Inc., Apple Inc., Sony Corp., Canon Inc., International Business Machines (IBM) Corp., Samsung Electronics Co. Ltd, Symantec Corporation, and Lucent Technologies, Inc., and banks like Bank of America Corporation and Wells Fargo Bank, N.A.

8. The 905 Patent overcame a rejection under 35 U.S.C 101 at the U.S. Patent and Trademark Office (the "Office" or "USPTO") that the invention was directed to a judicial exception (*i.e.*, to an abstract idea) without reciting "significantly more." Specifically, the applicant traversed the rejection by arguing that contrary to the Office's position, the claims were not directed to an abstract idea under step 2A of the *Alice/Mayo* eligibility test as "they disclose security scheme selection on a per-user basis which is available to users of the same computer system so that individual users can select his or her own authentication method for accessing the computer system, which is a concrete improvement in the field, particularly in view of the filing date of the subject application." The applicant further argued that "even if the claims were directed to an abstract idea, which is a point not conceded by Applicant, Applicant submits that the pending claims provide 'significantly more' under step 2B of the *Alice/Mayo* test by enabling individual users to select their own particular security scheme along with the system's ability to support different amounts of identification information to satisfy each selected security scheme, on a per-user basis." "Stated another way, by way of explanation, each user of the computer system can choose the security scheme that best meets their personal preference for the amount of identification information that is required in order to authorize their access to the computer system, thereby implicitly providing users with control over the ***'strength'*** of the authorization scheme they wish to be used to prevent unauthorized third-party access."

9. The applicant further argued that "[t]hese are technological improvements that were not 'well understood, routine, or conventional' at the time of filing." "Respectfully, the Office's step 2B position does not rebut this point, as the present Office Action lacks any factual basis to support a finding that the claims are well-understood, routine, or conventional as called for in the USPTO's own guidance of April 19, 2018." "In fact, Applicant asserts that a factual

basis exists in the case law to find oppositely that the claims are unconventional, namely that the pending claims are generally analogous to those found patent eligible under Step 2B in *Bascom Global Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341, 1350 (Fed. Cir. 2016)." "In Bascom, the patentee satisfied the 'significantly more' test by harmonizing two known, conventional filtering schemes into a new process, and the features of the claims now pending are fairly understood as satisfying the 'significantly more' test in the same way by providing a specific improvement in the form of a user-customizable authorization process for accessing a computer system." Applicant's request for reconsideration and withdrawal of the rejection under 35 U.S.C. 101 was well taken, as the rejection of the claims under 35 U.S.C. 101 was traversed and the Patent Office allowed the claims for issuance as a patent, closing prosecution on the merits.

FACTUAL ALLEGATIONS

I. TECHNOLOGY BACKGROUND

10. The application that led to the 905 Patent was filed in 1999. At that time, computer access security systems limited each and every user to a single secure authorization scheme, such scheme being administered ***system-wide***. That is, each user did not even have a choice because there was only a single method for secure system access authorization, namely the single security scheme that the computer system had been programmed to utilize. By way of example, to authorize a user, systems of that era required a fixed number of identification information to authorize that user for access to the system. By way of explanation, a user could not select an alternative security scheme to bolster the "strength" of the default security scheme - *e.g.*, a user could not request additional security by configuring the system to require additional identification information beyond that of the system's fixed number of identification information.

II. CODIGNOTTO'S INNOVATIVE TECHNOLOGY

11. Inventor John Codignotto recognized the problems with existing single-method access authorization systems and their lack of customization. The claims of the 905 Patent solved these problems and thereby improved the technical field by giving individual users the ability to select from **a plurality** of security schemes. Among the schemes that are selectable, at least one requires a different number of identification information than another scheme, to thereby enable--by way of explanation--individual users to prioritize either authorization strength or convenience in their selection of a computer access security scheme. By way of explanation, the independent claims 1 and 9 disclose a methodology in which an individual user can select either a (first) less secure, but less demanding to authorize, security scheme *(i.e.,* one requiring a specific number of identification information in order for the security scheme to be satisfied) or a (second) more secure, but more demanding to authorize, security scheme for authorization *(i.e.,* one requiring additional identification information beyond that of the first scheme in order for the second security scheme to be satisfied, as recited in claim 1, or that a different number of identification information be provided as recited in claim 9). The selection of preferences is **stored** in the particular user's storage area on the computer system and thereafter used to authorize that particular user's access to the system.

12. Claims like those of the 905 Patent, which improve a technology or technological field, as is the case here, are patent eligible as being **not** directed to abstract ideas under Step 2A of the *Alice/Mayo* eligibility test. *See* MPEP 2106.0S(a)(II); *McRO v. Bandai Namco Games Am. Inc.,* 837 F.3d 1299, 1310 (Fed. Cir. 2016) (claims that "effect an improvement in [a] technology or technical field" are eligible); *Enfish, LLC v. Microsoft Corp.,* 822 F.3d 1327, 1337 (Fed. Cir. 2016) (claims found eligible for achieving benefits over conventional databases, thereby

improving existing technology); *Trading Techs. Int 'l, Inc. v. CQG, Inc*., 675 Fed. Appx. 1001 (Fed. Cir. 2017) (method and system for electronic trading imparts a specific functionality that improves the accuracy of trader transactions).

13. Furthermore, the solution claimed in the 905 Patent does not simply use computers to serve a conventional business purpose, rather, they are "necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks," which is a base of patent eligibility articulated in *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1257 (Fed. Cir. 2014). As identified above, the technology at the time of filing limited each and every user to a single secure authorization scheme that was administered system-wide. The claims, however, provide individual users with the ability to select from a plurality of security schemes, and each security scheme can be understood, by way of explanation, as having a different "strengths," which directly overcomes these limitations inherent in the technology.

14. In addition to improving the technological field by providing individual users the ability to select a security scheme to be used to authorize their respective access to a computer system, the concepts embodied by Applicant's claims are meaningfully different than abstract ideas such as secure user authorization. Specifically, the claims disclose features in which different users are permitted to select different security schemes from one another, such schemes requiring a different number of identification information to authorize each user, all to access the same computer system, effectively can be understood as having different "strengths," by way of explanation. This is not analogous to, for example, characterization of a simple secure user authorization and collection of user account information. As that concept was implemented in

1999, all users were limited to the ***same*** security scheme offered by the system, and thus each user was forced to use the ***same*** security scheme provided to all users by the computer system.

15. Additionally, at the time of priority, the claimed features were not "well-understood, routine, or conventional activities known in the industry." Specifically, the claims amount to "significantly more" than any abstract idea by harmonizing the twin concepts of: (1) supporting a variety of different security schemes by requiring for the several schemes different amounts of identification information, which, in essence and by way of explanation, imparts each scheme with a comparatively stronger or weaker overall authorization, and (2) allowing individual selection and storage of a user-selected security scheme from among several security scheme choices. In 1999, well-understood, conventional and routine computer access authorization systems were limited to a single, system-wide security scheme that the system was programmed to utilize/perform (i.e., conventional computer access security systems did not offer security schemes that varied in the number of identification information required to authorize a user and, consequently, by way of explanation, varied the inherent "strength" of the computer access authorization, and they did not offer the ability for users to select their own security scheme from among a plurality of security schemes). The claims address these drawbacks by harmonizing these twin concepts, thereby setting forth an inventive concept that amounts to significantly more than any asserted abstract idea.

16. The claims also improve upon conventional computer access security by adding the **unconventional** ability of supporting a plurality of system access security schemes. The claims **also** add the **unconventional** ability of enabling individual users to select their own system access security scheme instead of the conventional approach in which users are forced to

use a scheme dictated by a third party, such as a system administrator, or are otherwise constrained by the limitations of conventional single-scheme computer access security systems.

17. The claims as a whole are directed to a non-abstract, concrete, technological improvement which imparts significantly more to a function of a conventional computer system.

III. INFRINGEMENT ALLEGATIONS

18. Socketlabs allows users to access the Socketlabs service that runs on computer systems operated by Socketlabs. Access to a Socketlabs account is authorized by a particular user providing identification information.

19. Socketlabs has manufactured, used, marketed, distributed, sold, offered for sale, exported from, and imported into the United States, products that infringe the 905 Patent. These Accused Products include at least all versions and variants of the Socketlabs Website since 2019. The Accused Products provide access to the Socketlabs platform, which includes email analytics and delivery.

20. The Accused Products have, since at least 2019, infringed the 905 Patent in allowing each particular user to customize the security scheme of their respective access to the system. Users can select between a standard username and password security scheme (i.e., Two-Step Verification is not enabled), and for a two-factor security scheme that requires an additional piece of identification information to authorize the user to access their account on the system, independent of the security scheme selected by other users of the Socketlabs system. See e.g., https://web.archive.org/web/20190402171749/https://help.socketlabs.com/docs/two-step-verification. Quotes from relevant portions of the Socketlabs website taken on April 2, 2019, as captured by the Internet Archive Wayback Machine, are reproduced below:

Two-Step Verification

What Is Two-Step Verification?

Two-step Verification is one of Socketlabs' additional security features. It prevents unauthorized users from logging into your Socketlabs Control Panel even if they have acquired your username and password.

It does this by using one of your personal devices to verify your identity. When you set up two-step verification, you register a device with us that you know you will be able to access whenever you are logging in. This device can be a smartphone, tablet, laptop or desktop computer, really any device that can receive SMS or on which a Google Authenticator application can be installed.

Every time you attempt to log into the Socketlabs Control Panel, a special verification code will be sent to your device via SMS or Google Authenticator. This verification code must then be entered to complete the login process. Without your personal device, no one else can access your account!

How Do I Set Up Two-Step Verification?

Each user can set up Two-Step Verification for their individual account by taking the following actions.

- Log into the Socketlabs Control Panel.
- Click on your name in the upper right-hand corner of the screen.
- Select Security from the drop-down menu.
- Click on the blue Enable Two-Step Verification button.

- This will bring up a setup wizard. Simply follow the instructions, which will walk you through each step.

Please note that once you complete this process, you will be required to verify your identity using two-step authentication every time you log in.

What If I Can't Access The Device I Use For Two-Step Verification?

Sometimes a phone gets lost or stolen, a computer becomes non-functional, you leave a device behind when going on vacation, or any of a thousand little things can happen to prevent you from accessing your device. We understand this and therefore provide a couple of backup options for accessing your account when the primary method you selected is unavailable.

Backup Phone Number

During Two-Step Verification setup, you will be presented with the option to provide a backup phone number for verification via SMS. You can also provide this at a later time by viewing the Security page and selecting "Add a backup phone number". When you are asked for a verification code while logging into Socketlabs' Control Panel, click on the "Having trouble?" link and then select "Send a verification code to my backup phone number ending with XXXX". This will allow you to enter a code sent to your backup phone.

Backup Codes

When you set up Two-Step Verification, we provide you with a set of printable, one-time-use Backup Codes. When you are asked for a verification code while logging in, click on the "Having trouble?" link and then select "Let me enter one of my backup codes". Remember: each of these codes are usable one time only. We recommend keeping this list in a secure location and crossing any codes you have used off of your list.

If you use the last of your Backup Codes, do not log out without navigating to the Security page and selecting "Regenerate backup codes"! This will provide you with a whole new set.

How Do I Turn Off Two-Step Verification?

To turn off Two-Step Verification for your user account, follow the instructions below.

- Log into the Socketlabs Control Panel.
- Click on your name in the upper right-hand corner of the screen.
- Select Security from the drop-down menu.
- Click on the orange Remove Two-Step Verification button.
- Click Yes in the pop-up to confirm that you definitely wish to disable Two-Step Verification.

If you are the account owner, you can see whether or not Two-Step Verification is enabled for each particular user on the same account. Should you need to turn off Two-Step Verification for another user, follow these instructions.

> - Log into the Socketlabs Control Panel.
> - Click on the Users button near the upper left-hand corner.
> - Select the Edit button next to the appropriate user.
> - Click on the Remove button next to the user's Two-Step Verification status.
> - Click OK in the pop-up to confirm that you definitely wish to disable Two-Step Verification for this user.
>
> **How Do I Change My Two-Step Verification Device Or Method?**
>
> You may change your Two-Step Verification settings at any time by navigating to the Security page and clicking Edit next to the phone number you wish to change. You may also click Remove next to the Backup number if you no longer wish to provide a secondary device.
>
> If you have enabled SMS verification and wish to switch to Google Authenticator (or vice versa), simply Remove your existing configuration and then click Enable Two-Step Verification to begin again.
>
> Google Authenticator must be set up anew for each new device.

21. On information and belief, the Accused Products are made available via Socketlabs's computer system (*i.e.*, plurality of servers), which has a plurality of user accounts each with a respective storage area.

22. The Accused Products prompt users to select a security scheme within the Socketlabs user interface by offering a security settings prompt.

23. On information and belief, the user's security scheme choice (*i.e.* whether to use two factor authentication or not) is stored in the user's storage area so that the system will know which security scheme is to be used when the user attempts to access the system.

24. The first security scheme (*i.e*, Two-Step Verification is not enabled) requires just two pieces of identification information; a username and a password.

25. The second security scheme as explained by Socketlabs, requires the same two pieces of identification information (a username and a password), plus a third piece of identification information, the two-factor authentication code.

26. As discussed above, on information and belief, as reflected in the above link, after the user selects a particular security scheme, that scheme is used in each subsequent login by the user, indicating that the selection is stored as a preference in the user's storage area.

27. If the user did not enable Two Factor Security authentication, then just the user's username and password is required to satisfy the first security scheme and allow the user to access the system. However, if the user enabled Two Factor Security authorization, the user must then additionally provide a third piece of identification information (the two-factor code) to satisfy the second security scheme and access the system, as shown below.

<u>COUNT I – INFRINGEMENT OF U.S. PATENT NO. 10,114,905</u>

28. Plaintiff repeats and realleges all preceding paragraphs, as if fully set forth herein.

29. Plaintiff has not licensed or otherwise authorized Socketlabs to make, use, offer for sale, sell, or import any products that embody the inventions of the 905 Patent.

30. Socketlabs directly infringes at least claims 1-20 of the 905 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that

satisfy each and every limitation of one or more claims of the 905 Patent. These products include at least all versions and variants of Socketlabs Website.

31. For example, Socketlabs directly infringes at least claims 1-20 by making, using, offering to sell, selling, and/or importing into the United States products with user customizable access security. Using Socketlabs's servers, the Accused Products utilize various user-selectable access security schemes as described above, and infringe the claims of the 905 Patent.

32. The infringing aspects of the Accused Products can be used only in a manner that infringes the 905 Patent and thus have no substantial non-infringing uses. The infringing aspects of those instrumentalities otherwise have no meaningful use, let alone any meaningful non-infringing use.

33. Socketlabs indirectly infringes one or more claims of the 905 Patent by knowingly and intentionally inducing others, including Socketlabs customers and end-users of the Accused Products and products that include the Accused Products, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as the Socketlabs Website.

34. Socketlabs has indirectly infringed one or more claims of the 905 Patent, as provided by 35 U.S.C. § 271(b), by inducing infringement by others, such as Socketlabs's customers and end-users, in this District and elsewhere in the United States. For example, Socketlabs's customers and end-users directly infringe, either literally or under the doctrine of equivalents, through their use of the inventions claimed in the 905 Patent. Socketlabs induces this direct infringement through its affirmative acts of manufacturing, selling, distributing, and/or otherwise making available the Accused Products, and providing instructions, documentation,

and other information to customers and end-users suggesting that they use the Accused Products in an infringing manner, including technical support, marketing, product manuals, advertisements, and online documentation. Because of Socketlabs's inducement, Socketlabs's customers and end-users use the Accused Products in a way Socketlabs intends and directly infringe the 905 Patent. Socketlabs performs these affirmative acts with knowledge of the 905 Patent and with the intent, or willful blindness, that the induced acts directly infringe the 905 Patent.

35. Socketlabs has indirectly infringed one or more claims of the 905 Patent, as provided by 35 U.S.C. § 271(c), by contributing to direct infringement by others, such as customers and end-users, in this District and elsewhere in the United States. Socketlabs's affirmative acts of selling and offering to sell the Accused Products in this District and elsewhere in the United States and causing the Accused Products to be manufactured, used, sold and offered for sale contributes to others' use and manufacture of the Accused Products, such that the 905 Patent is directly infringed by others. The accused components within the Accused Products are material to the invention of the 905 Patent, are not staple articles or commodities of commerce, have no substantial non-infringing uses, and are known by Socketlabs to be especially made or adapted for use in the infringement of the 905 Patent. Socketlabs performs these affirmative acts with knowledge of the 905 Patent and with intent, or willful blindness, that they cause the direct infringement of the 905 Patent.

36. Plaintiff has been injured and seeks damages to adequately compensate it for Socketlabs's infringement of the 905 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

DEMAND FOR JURY TRIAL

Plaintiff hereby requests a jury trial of all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for relief against Defendant as follows:

a. Entry of judgment declaring that Defendant has directly and/or indirectly infringed one or more claims of the Patent-in-Suit;

b. An order awarding damages sufficient to compensate Plaintiff for Defendant's infringement of the Patent-in-Suit, but in no event less than a reasonable royalty, including supplemental damages post-verdict, together with pre-judgment and post-judgment interest and costs;

c. Entry of judgment declaring that this case is exceptional and awarding Plaintiff its costs and reasonable attorney fees pursuant to 35 U.S.C. § 285;

d. An accounting for acts of infringement;

e. Such other equitable relief which may be requested and to which the Plaintiff is entitled; and

f. Such other and further relief as the Court deems just and proper.

Dated: November 25, 2024

Respectfully submitted,

/s/David L. Hecht
David L. Hecht
dhecht@hechtpartners.com
HECHT PARTNERS LLP
125 Park Avenue, 25th Floor
New York, New York 10017
Telephone: (212) 851-6821

Counsel for Plaintiff EasyWeb Innovations, LLC