UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

GUYZAR LLC, Plaintiff, v. **GOLD'S GYM INTERNATIONAL, INC.**, Defendant.	**CIVIL ACTION NO.** **DEMAND FOR JURY TRIAL**

COMPLAINT FOR INFRINGEMENT OF PATENT

COMES NOW, Plaintiff Guyzar LLC ("Guyzar" or Plaintiff), through the undersigned attorneys, 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 Gold's Gym International, Inc. (hereinafter "Gold") from infringing and profiting, in an illegal and unauthorized manner and without authorization or of the consent from Guyzar, from U.S. Patent No. 5,845,070 (the "'070 Patent," attached hereto as Exhibit "A") pursuant to 35 U.S.C. § 271, and to recover damages, attorney's fees, and costs.

THE PARTIES

2. Plaintiff Guyzar LLC is a Texas entity with its principal place of business at 5700 Granite Parkway, Suite 200, Plano, TX 75024.

3. Upon information and belief, Defendant is a corporation organized and existing under the laws of Delaware, with a principal place of business at 125 East John Carpenter Freeway, Suite 1300, Irving, TX 75062.

JURISDICTION AND VENUE

4. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1338(a) because the action arises under the Patent Laws of the United States, 35 U.S.C. §§ 1 et seq.

5. Defendant is subject to this Court's personal jurisdiction pursuant to due process or the Delaware Long Arm Statute, due at least to its substantial business and purposeful availment of 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, or deriving substantial revenue from goods and services provided to individuals in Delaware and in this judicial district. Defendant is also incorporated in this District.

6. Upon information and belief, Defendant, directly or through its end-users, uses the accused instrumentalities, as defined below, with the knowledge or understanding that such accused devices will be used in this District. For example, the accused instrumentality is used in this District through Defendant's website. Upon information and belief, Defendant has engaged in substantial and not isolated activity within this District. Therefore, exercise of jurisdiction over Defendant will not offend traditional notions of fair play and substantial justice. Such an exercise is consistent with the Delaware long-arm statute.

7. Venue is proper in this judicial district pursuant to § 1400(b) because Defendant is incorporated in this state, is subject to personal jurisdiction in this district,

has regularly conducted business in this judicial district and certain of the acts complained of herein occurred in this judicial district.

FACTUAL ALLEGATIONS

8. On December 1, 1998, the United States Patent and Trademark Office ("USPTO") duly and legally issued the '070 Patent, entitled "Security System for Internet Provider Transaction" after a full and fair examination.

9. Guyzar includes a true, accurate, correct, and legible copy of the '070 Patent as Exhibit A of this Complaint and incorporates it by reference herein, making it part of the Complaint for all legal, procedural, or evidentiary purposes.

10. Guyzar is presently the owner of the Patent, having received all right, title and interest in and to the '070 Patent from the previous assignee of record. Guyzar possesses all rights of recovery under the '070 Patent, including the exclusive right to recover for past infringement.

11. The '070 Patent contains three (3) independent claims and ten (10) dependent claims. Defendant commercializes, *inter alia*, methods that perform all the steps recited in at least one claim of the '070 Patent.

12. The invention claimed in the '070 Patent comprises a method of authenticating a user's confidential information and preserving the confidentiality against unauthorized use, said information being essential for conducting Internet transactions between a log-in and log-out session.

DEFENDANT'S PRODUCTS

13. Guyzar incorporates the above paragraphs herein by reference.

14. Gold has been and continues to directly infringe at least Claim 1 of the '070 Patent in this District and elsewhere in the United States by performing the steps of "authenticating a user's confidential information and preserving the confidentiality against unauthorized use, said information being essential for conducting Internet transactions between a log-in and log-out session." For example, Gold's website includes features, such as the "Sign In" Feature (the "Accused Instrumentality") shown below, that allow for the authentication of a user's confidential information and for the preservation of the confidentiality of said information against unauthorized use, said information being essential for conducting Internet transactions between a log-in and log-out session. Further, the Accused Instrumentality utilizes the OAuth open standard to provide a method of authenticating a user's confidential information and preserving said confidential information against unauthorized use as recited by at least the preamble of Claim 1 of the '070 Patent. *See* Figures 1–3.

Logging into another site with your Google, Twitter, or Facebook account isn't just convenient; it's more secure than creating a new account, or entering your Google, Twitter, or Facebook password into a third-party site. That's where OAuth comes in. Here's how it works, and how it keeps your passwords safe on third-party sites.

Yesterday, a Twitter app called Tweetgif was hacked, releasing user information for 10,000 Twitter accounts to the public. However, no Twitter credentials were compromised, because Tweetgif used something called OAuth. If you've ever logged into a third-party web site with your Google, Facebook, or Twitter account by granting the app permission to that respective account, then whether you knew it or not, you've used OAuth, and it's a great way to dole out permissions.

Figure 1. OAuth is a delegation protocol that is used for conveying authorization decisions across a network of applications and APIs in a secure manner.

Available at: http://lifehacker.com/5918086/understanding-oauth-what-happens-when-you-log-into-a-site-with-google-twitter-or-facebook.

OAuth addresses these issues by introducing an authorization layer and separating the role of the client from that of the resource owner. In OAuth, the client requests access to resources controlled by the resource owner and hosted by the resource server, and is issued a different set of credentials than those of the resource owner.

Instead of using the resource owner's credentials to access protected resources, the client obtains an access token -- a string denoting a specific scope, lifetime, and other access attributes. Access tokens are issued to third-party clients by an authorization server with the approval of the resource owner. The client uses the access token to access the protected resources hosted by the resource server.

For example, an end-user (resource owner) can grant a printing service (client) access to her protected photos stored at a photo-sharing service (resource server), without sharing her username and password with the printing service. Instead, she authenticates directly with a server trusted by the photo-sharing service (authorization server), which issues the printing service delegation-specific credentials (access token).

Figure 2. The OAuth protocol provides a method of authenticating a user's third-party log-in credentials on the Defendant's website or app.

Available at: http://tools.ietf.org/html/rfc6749#section-1.2.

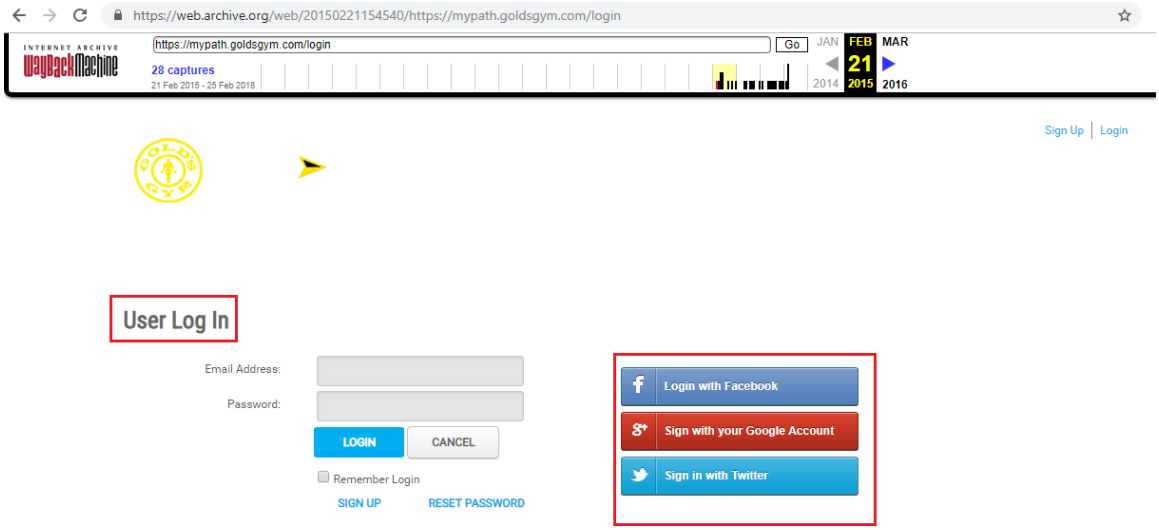
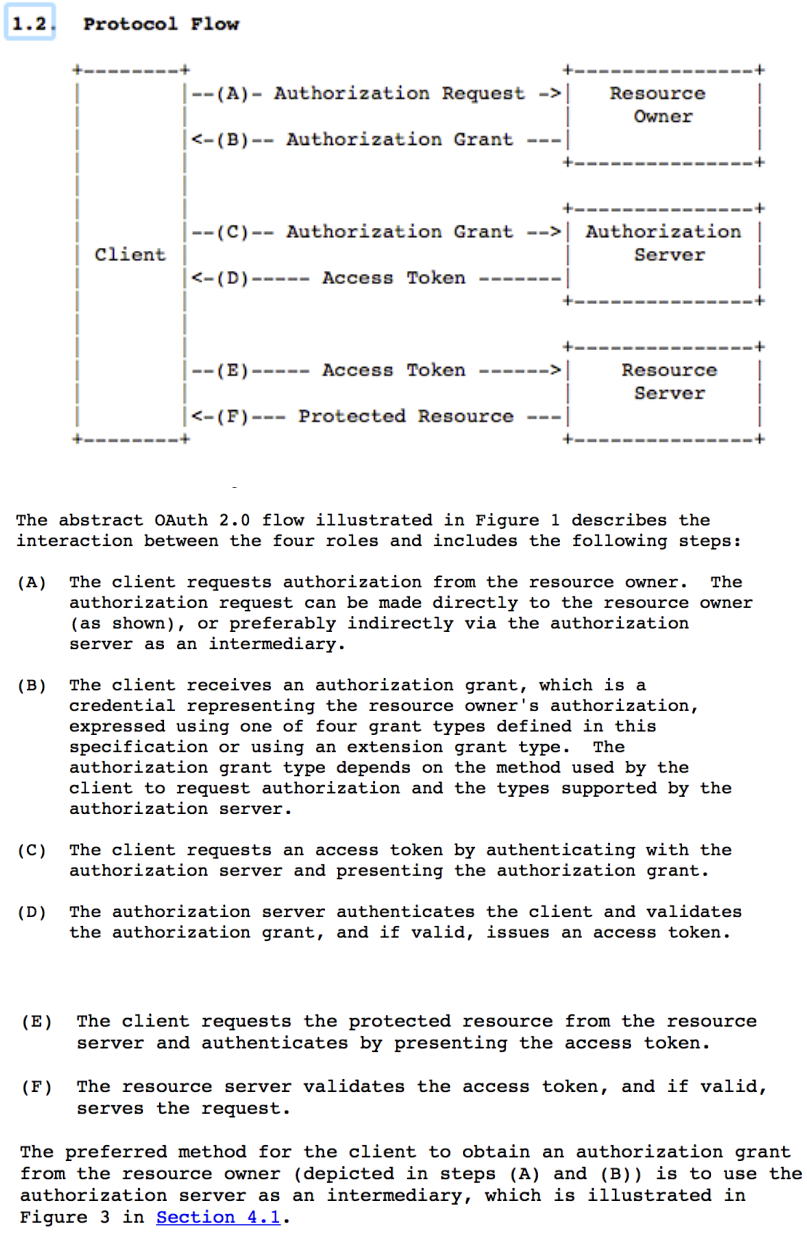


Figure 3. The Accused Product utilizes the OAuth open standard in providing a method of authenticating a user's confidential information (e.g. the OAuth protocol provides a method of authenticating a user's third-party log-in credentials on the Defendant's website or app) and preserving the confidentially of a user's Confidential information

against unauthorized use (e.g. a user's third party log-in credentials are kept confidential from the Defendant's website or app; while addresses, emails, phone numbers, online profiles, etc., that are linked to the log-in credentials are securely shared with the Defendant's website or app).

Available at:
https://web.archive.org/web/20150221154540/https://mypath.goldsgym.com/login.



1.2. Protocol Flow

```
+--------+                                +---------------+
|        |--(A)- Authorization Request ->|   Resource    |
|        |                               |     Owner     |
|        |<-(B)-- Authorization Grant ---|               |
|        |                               +---------------+
|        |
|        |                               +---------------+
|        |--(C)-- Authorization Grant -->| Authorization |
| Client |                               |     Server    |
|        |<-(D)----- Access Token -------|               |
|        |                               +---------------+
|        |
|        |                               +---------------+
|        |--(E)----- Access Token ------>|    Resource   |
|        |                               |     Server    |
|        |<-(F)--- Protected Resource ---|               |
+--------+                               +---------------+
```

The abstract OAuth 2.0 flow illustrated in Figure 1 describes the interaction between the four roles and includes the following steps:

(A) The client requests authorization from the resource owner. The authorization request can be made directly to the resource owner (as shown), or preferably indirectly via the authorization server as an intermediary.

(B) The client receives an authorization grant, which is a credential representing the resource owner's authorization, expressed using one of four grant types defined in this specification or using an extension grant type. The authorization grant type depends on the method used by the client to request authorization and the types supported by the authorization server.

(C) The client requests an access token by authenticating with the authorization server and presenting the authorization grant.

(D) The authorization server authenticates the client and validates the authorization grant, and if valid, issues an access token.

(E) The client requests the protected resource from the resource server and authenticates by presenting the access token.

(F) The resource server validates the access token, and if valid, serves the request.

The preferred method for the client to obtain an authorization grant from the resource owner (depicted in steps (A) and (B)) is to use the authorization server as an intermediary, which is illustrated in Figure 3 in Section 4.1.

Figure 4. Gold's Accused Instrumentality uses the OAuth standard to request and receive authorization from the resource owner. Access token are then granted and issued once

the authorization server validates the authenticity of the authorization grant and authenticates the client.

15. Gold's Accused Instrumentality has claim element 1(a): "accessing the Internet by the user entering a first data set into a computer based controller to control modems and communication protocols." For example, Gold's Accused Instrumentality accesses the Internet by having the user entering a first data set, such as third-party log-in credentials, into a computer-based controller to control modems and communication protocols as recited by at least the first element of Claim 1 of the '070 Patent. *See* Figure 5.

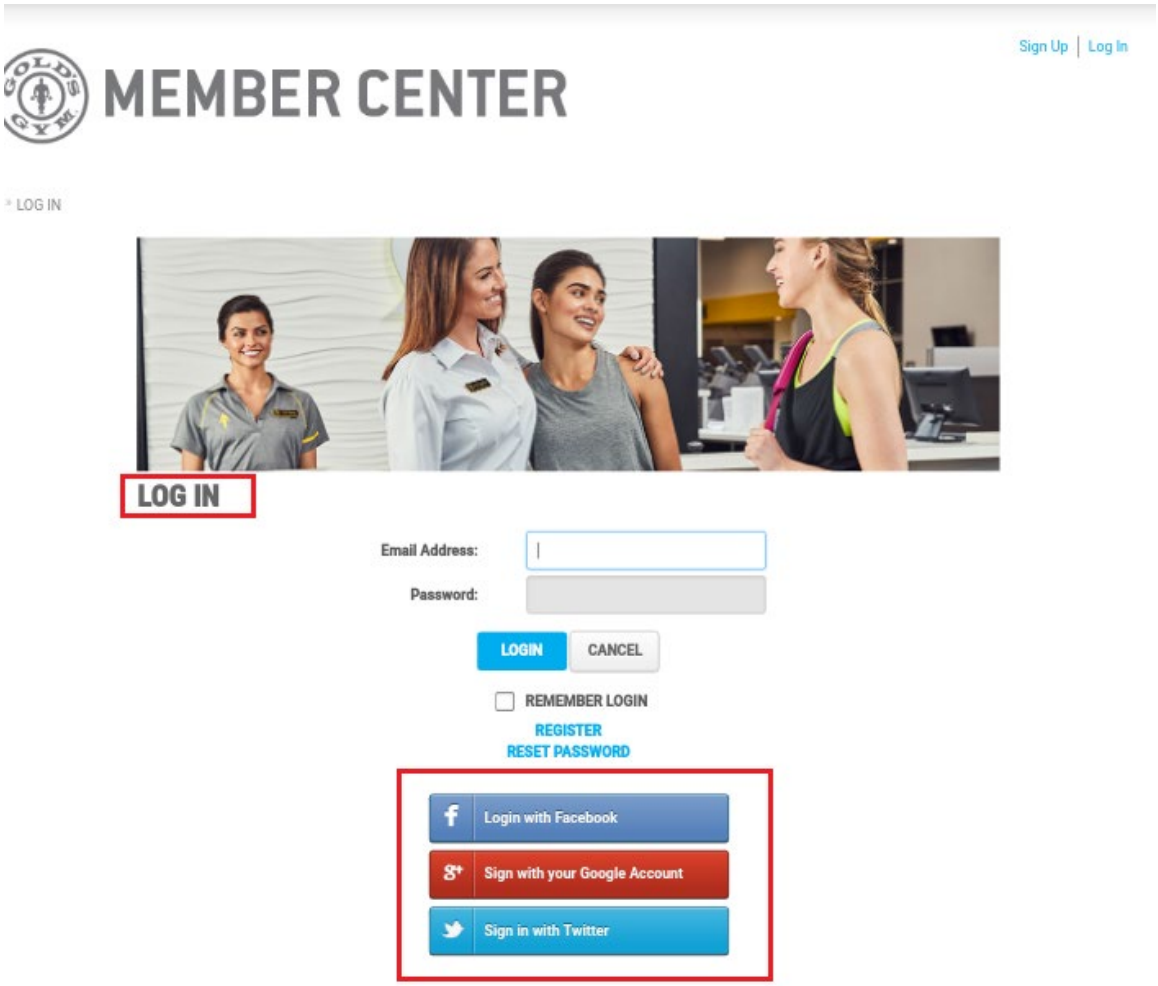


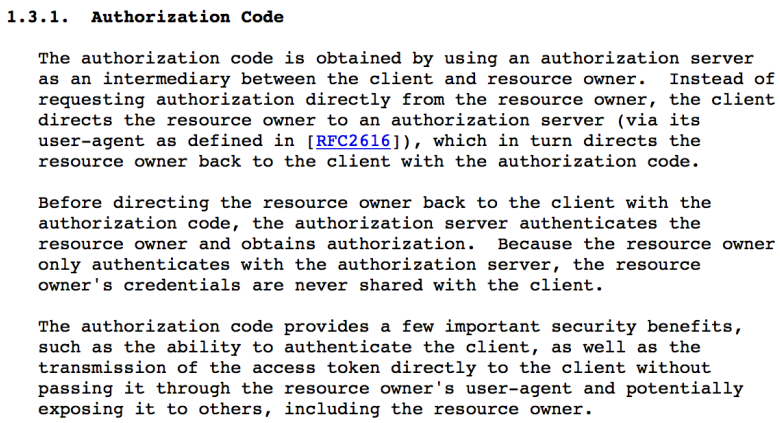
Figure 5. Gold's Accused Instrumentality allows users to sign in through a third-party platform, including: Facebook, Google and Twitter, for example.

16. Gold's Accused Instrumentality has claim element 1(b): "establishing a data base containing confidential information subject to authentication with a user's first data set." For example, Gold's Accused Instrumentality utilizes the OAuth standard to establish a database containing confidential information, such as (but not exclusively) a user's address, email, phone number, online profile, etc. subject to authentication with a user's first data set, as recited by at least the second element of Claim 1 of the '070 Patent. *See* Figures 4-5.

17. Gold's Accused Instrumentality has claim element 1(c): "submitting said first data set to a tracking and authentication control module requesting authentication of the user, said tracking and authentication control module including a data base containing user's confidential information, an authentication server for authenticating said first data set and a certification server, said certification server containing validation data for authenticating and internet entity approved for conducting internet transaction." For example, Gold's Accused Instrumentality implements the OAuth standard to submit a first data set to a tracking and authentication control module, such as a dedicated "Authorization Server," that requests authentication of the user said tracking and authentication control module including a database containing user's confidential information, such as the database established in an Authorization Server and Resource Server of the Accused Instrumentality, an authentication server for authenticating said first data set, and a certification server, said certification server containing validation data for authenticating and internet entity approved for conducting internet transactions, as recited by at least the third element of Claim 1 of the '070 Patent. *See* Figure 4.

18. Gold's Accused Instrumentality has claim element 1(d): "comparing the user's first data set input to the authentication server incident to accessing the internet with the I.D. and password in the data base and subject to a validating match." For example, Gold's Accused Instrumentality implements the OAuth standard to compare the user's first data set input to the authentication server incident to accessing the internet with the I.D. and password in the data base and subject to a validating match, as recited by at least the fourth element of Claim 1 of the '070 Patent. *See* Figure 4.

19. Gold's Accused Instrumentality has claim element 1(e): "issuing a second data set in real time by the authentication server subject to a validation match of the I.D. and password with the data in the database usable for the instant transaction." For example, Gold's Accused Instrumentality implements the OAuth standard in issuing a second data set, such as an Access Token and Authorization Code issued by the OAuth protocol, responsive to a successful validation of the I.D. and password with data in the database usable for the transaction, as recited by at least the fifth element of Claim 1 of the '070 Patent. *See* Figures 4, 6.

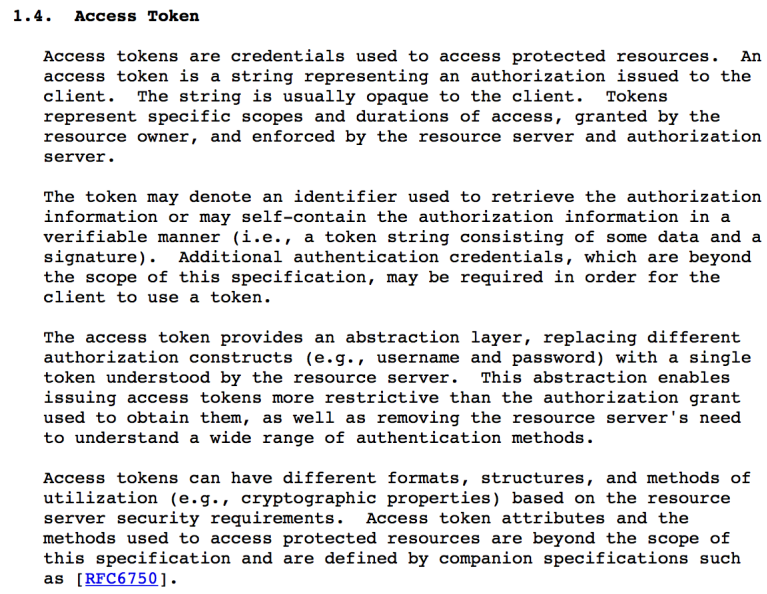


1.3.1. Authorization Code

The authorization code is obtained by using an authorization server as an intermediary between the client and resource owner. Instead of requesting authorization directly from the resource owner, the client directs the resource owner to an authorization server (via its user-agent as defined in [RFC2616]), which in turn directs the resource owner back to the client with the authorization code.

Before directing the resource owner back to the client with the authorization code, the authorization server authenticates the resource owner and obtains authorization. Because the resource owner only authenticates with the authorization server, the resource owner's credentials are never shared with the client.

The authorization code provides a few important security benefits, such as the ability to authenticate the client, as well as the transmission of the access token directly to the client without passing it through the resource owner's user-agent and potentially exposing it to others, including the resource owner.



1.4. Access Token

Access tokens are credentials used to access protected resources. An access token is a string representing an authorization issued to the client. The string is usually opaque to the client. Tokens represent specific scopes and durations of access, granted by the resource owner, and enforced by the resource server and authorization server.

The token may denote an identifier used to retrieve the authorization information or may self-contain the authorization information in a verifiable manner (i.e., a token string consisting of some data and a signature). Additional authentication credentials, which are beyond the scope of this specification, may be required in order for the client to use a token.

The access token provides an abstraction layer, replacing different authorization constructs (e.g., username and password) with a single token understood by the resource server. This abstraction enables issuing access tokens more restrictive than the authorization grant used to obtain them, as well as removing the resource server's need to understand a wide range of authentication methods.

Access tokens can have different formats, structures, and methods of utilization (e.g., cryptographic properties) based on the resource server security requirements. Access token attributes and the methods used to access protected resources are beyond the scope of this specification and are defined by companion specifications such as [RFC6750].

Figure 6. Gold's Accused Instrumentality implements the OAuth standard in issuing a second data set, such as an Access Token and Authorization Code issued by the OAuth protocol, responsive to a successful validation of the I.D. and password with data in the database usable for the transaction.

Available at: http://tools.ietf.org/html/rfc6749#section-1.2.

20. Gold's Accused Instrumentality has claim element 1(f): "submitting the second data set to the certification server upon the initiation of the transaction by the user." For example, Gold's Accused Instrumentality implements the OAuth standard to submit the second data set to the certification server upon initiation of a transaction by the user. Further, the Resource Server of the Accused Instrumentality serves its certification purpose and validates the authenticity of the Access Token before allowing Defendant's website to access the user's confidential information upon initiation of a transaction by the user, as recited by at least the sixth element of Claim 1 of the '070 Patent. *See* Figures 4.

21. Gold's Accused Instrumentality has claim element 1(g): "consummating the transaction subject to validation of the second data set by typing the confidential

information in the data base to the user whereby the confidential information is retained undisclosed in the data base." For example, Gold's Accused Instrumentality implements the OAuth standard in consummating a transaction, such as using user's third-party credentials and profile information on Defendant's website, subject to the validation of the second data set by tying the confidential information in the data base to the user whereby the confidential information is retained undisclosed in the database, as recited by at least the seventh element of Claim 1 of the '070 Patent. *See* Figures 4, 6.

22. The elements described in paragraphs 13-21 are covered by at least Claim 1 of the '070 Patent. Thus, Defendant's use of the Accused Instrumentality, including the use by Defendant's end-users and employees, is enabled by the process described in the '070 Patent.

23. Defendant conditions end-users' use of the Accused Instrumentality upon the end users' and Facebook's performance of the method recited herein. That is, if end-users wish to use the Accused Instrumentality they (in combination with Facebook) must perform the steps recited in at least Claim 1. This is because by implementing the OAuth standard the Accused Instrumentality performs each step recited in, at least, Claim 1.

24. Defendant establishes the manner or timing of end-users' performance of the claimed method. That is, if end-users do not follow the claimed steps, Defendant's service (i.e., logging in without end-user having to share email/password) will not be available. Thus, the infringement of these third parties is attributable to Defendant.

INFRINGEMENT OF THE '070 PATENT

25. Plaintiff realleges and incorporates by reference the allegations set forth in

paragraphs 1 to 23.

26. In violation of 35 U.S.C. § 271, Defendant is now, and has been directly infringing the ’070 Patent.

27. Defendant has had knowledge of infringement of the ’070 Patent at least as of the service of the present complaint.

28. Defendant has directly infringed and continues to directly infringe at least Claim 1 of the ’070 Patent by using the Accused Instrumentality which allows end-users to log in and make their respective purchases or access their services, without authority in the United States, during the period in which the ’070 Patent was unexpired, causing damages to Plaintiff for that period of time. Upon information and belief, Gold directly infringes both by using and internally testing it. *See* Figures 1-5.

29. By engaging in the conduct described herein, Defendant has injured Guyzar and is thus liable for infringement of the ’070 Patent, pursuant to 35 U.S.C. § 271.

30. Defendant has committed these acts of infringement without license or authorization.

31. As a result of Defendant’s infringement of the ’070 Patent, Guyzar has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate for Defendant’s past infringement, together with interests and costs.

32. Guyzar is entitled to recover damages adequate to compensate it for such infringement in an amount no less than a reasonable royalty under 35 U.S.C. § 284.

DEMAND FOR JURY TRIAL

33. Under Rule 38(b) of the Federal Rules of Civil Procedure, Guyzar demands a trial by jury of any and all causes of action.

PRAYER FOR RELIEF

WHEREFORE, Guyzar prays for the following relief:

a. That Defendant be adjudged to have infringed the '070 Patent, directly, literally or under the doctrine of equivalents;

b. An award of damages pursuant to 35 U.S.C. § 284 sufficient to compensate Guyzar for the Defendant's past infringement, including compensatory damages;

c. 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;

d. An accounting of all damages not presented at trial;

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

f. That Guyzar have such other and further relief as this Court may deem just and proper.

Dated: November 19, 2018

Respectfully submitted,

/s/ Timothy Devlin
Timothy Devlin (#4241)
Devlin Law Firm LLC
1306 N. Broom St., Suite 1
Wilmington, DE 19806
302.449.9010
302.353.4251
tdevlin@devlinlawfirm.com

Isaac Rabicoff
(*Pro Hac Vice Admission Pending)*
Kenneth Matuszewski
(*Pro Hac Vice Admission Pending*)
RABICOFF LAW LLC
73 W Monroe St.
Chicago, IL 60603
(773) 669-4590
isaac@rabilaw.com
kenneth@rabilaw.com

Counsel for Plaintiff