

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE**

GUYZAR LLC,	:	
	:	
Plaintiff,	:	C.A. NO. 18-CV-01257 CFC
	:	
v.	:	DEMAND FOR JURY TRIAL
	:	
STUBHUB, INC.,	:	
	:	
Defendant.	:	

**OPENING BRIEF IS SUPPORT OF
DEFENDANT STUBHUB, INC.'S RULE 12(b)(6)
MOTION TO DISMISS FOR FAILURE TO STATE A CLAIM**

FISH & RICHARDSON P.C.
Jeremy D. Anderson (#4515)
222 Delaware Ave., 17th Floor
P.O. Box 1114
Wilmington, DE 19801
(302) 652-5070 (Telephone)
(302) 652-0607 (Facsimile)
janderson@fr.com

Neil J. McNabnayd
William B. Collier
1717 Main Street, Suite 5000
Dallas, TX 75201
(214) 747-5070 (Telephone)
(214) 747-2091 (Facsimile)
mcnabnay@fr.com
collier@fr.com

**COUNSEL FOR DEFENDANT
STUBHUB, INC.**

Dated: September 10, 2018

TABLE OF CONTENTS

I. INTRODUCTION1

II. NATURE AND STAGE OF PLEADINGS1

III. SUMMARY OF THE ARGUMENTS1

IV. STATEMENT OF THE FACTS2

 A. The patent-in-suit2

V. MOTION TO DISMISS PURSUANT TO 35 U.S.C. § 101.....3

 A. This case should be decided at pleading stage under Rule 12(b)(6).....3

 B. The law of 35 U.S.C. § 101.....4

 C. The '070 patent is patent-ineligible5

 1. Alice step one: the '070 patent is directed to an abstract idea.6

 (a) Confidentially authenticating users is an abstract idea.....6

 (b) Because the confidential transaction is untethered to a specific implementation, it is abstract.....8

 (c) Because the '070 patent claims are not directed to a specific improvement in a computer’s capabilities, they are abstract.11

 2. Alice step two: the '070 patent claims only implement the abstract idea of using generic computer technology, add nothing inventive, and are therefore patent-ineligible.13

 (a) The independent claims add nothing inventive.13

 (b) The dependent claims add nothing inventive.15

 (c) The '070 patent claims are patent-ineligible under any claim constructions.16

VI. MOTION TO DISMISS FOR FAILURE TO STATE A CLAIM17

 A. The law of Rule 121(b)(6).....17

B.	Guyzar has not pleaded sufficient detail to provide notice of its joint infringement allegations.....	18
VII.	CONCLUSION	20

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Akamai Techs., Inc. v. Limelight Networks, Inc.</i> , 797 F.3d 1020 (Fed. Cir. 2015).....	18
<i>Apple, Inc. v. Ameranth, Inc.</i> , 842 F.3d 1229 (Fed. Cir. 2016).....	9, 11
<i>Asghari-Kamrani v. United Servs. Auto Ass’n</i> , 2016 WL 3670804 (E.D. Va. Jul. 5, 2016).....	11, 16
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009).....	4, 17
<i>Bascom Global Internet Servs., Inc. v. AT&T Mobility LLC</i> , 827 F.3d 1341 (Fed. Cir. 2016).....	14, 15
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007).....	4, 17, 20
<i>Bilski v. Kappos</i> , 561 U.S. 593 (2010).....	4, 5, 7, 16
<i>buySAFE v. Google, Inc.</i> , 765 F.3d 1350 (Fed. Cir. 2014).....	14
<i>Collins v. Morgan Stanley Dean Witter</i> , 224 F.3d 496 (5th Cir. 2000).....	19
<i>Content Extraction and Transmission LLC v. Wells Fargo Bank, Nat’l Ass’n</i> , 776 F.3d 1343 (Fed. Cir. 2014).....	<i>passim</i>
<i>CyberSource Corp. v. Retail Decisions, Inc.</i> , 654 F.3d 1366 (Fed. Cir. 2011).....	5, 10
<i>Dealertrack, Inc. v. Huber</i> , 674 F.3d 1315 (Fed. Cir. 2012).....	9, 14, 16
<i>Diamond v. Chakrabarty</i> , 447 U.S. 303 (1980).....	4
<i>Elec. Power Group, LLC v. Alstom S.A.</i> , 830 F.3d 1350 (Fed. Cir. 2016).....	<i>passim</i>

Enfish, LLC v. Microsoft Corp.,
822 F.3d 1327 (Fed. Cir. 2016)..... 11, 12, 13

FairWarning IP, LLC v. Iatric Sys., Inc.,
839 F.3d 1089 (Fed. Cir. 2016)..... 10, 12

Fort Props., Inc. v. Am. Master Lease LLC,
671 F.3d 1317 (Fed. Cir. 2012)..... 5

Genetic Techs. Ltd. v. Merial L.L.C.,
818 F.3d 1369 (Fed. Cir. 2016)..... 4

Gines v. D.R. Horton, Inc.,
699 F.3d 812 (5th Cir. 2012)..... 19

Hartig Drug Co. v. Senju Pharm. Co.,
836 F.3d 261 (3d Cir. 2016)..... 4

Intellectual Ventures I LLC v. Capital One Bank (USA),
792 F.3d 1363 (Fed. Cir. 2015)..... 10, 14

Intellectual Ventures I LLC v. J. Crew Grp., Inc.,
2016 WL 4591794 (E.D. Tex. Aug. 24, 2016) 12

Intellectual Ventures I LLC v. Symantec Corp.,
838 F.3d 1307 (Fed. Cir. 2016)..... 9, 11, 15

Inventor Holdings, LLC v. Bed Bath & Beyond Inc.,
123 F. Supp. 3d 557 (D. Del. 2015)..... 8, 10

Lyda v. CBS Corp.,
838 F.3d 1331 (Fed. Cir. 2016)..... 17, 18

Mayo Collaborative Servs. v. Prometheus Labs., Inc.,
132 S. Ct. 1289 (2012) 5

McRO, Inc. v. Bandai Namco Games Am. Inc.,
837 F.3d 1299 (Fed. Cir. 2016)..... 11, 12

O2 Micro Intl. Ltd. v. Beyond Innovation Tech. Co.,
521 F.3d 1351 (Fed. Cir. 2008)..... 16

OpenTV, Inc. v. Apple, Inc.,
2015 WL 1535328 (N.D. Cal. Apr. 6, 2015) 11

Phoenix Licensing, L.L.C. v. Consumer Cellular, Inc.,
No. 2:16-cv-152-JRG-RSP, 2017 WL 1065938 (E.D. Tex. Mar. 8, 2017)..... 6

Pragmatus Telecomms., LLC v. Genesys Telecomms. Labs., Inc.,
114 F. Supp. 3d 192 (D. Del. 2015)..... 14, 15

Synopsys, Inc. v. Mentor Graphics Corp.,
839 F.3d 1138 (Fed. Cir. 2016).....15

In re TLI Communications LLC Patent Litigation,
823 F.3d 607 (Fed. Cir. 2016).....*passim*

Ultramercial, Inc. v. Hulu, LLC,
772 F.3d 709 (Fed. Cir. 2014) (Mayer, J., concurring) 4, 9, 16

Visual Memory LLC v. NVIDIA Corp.,
2017 WL 3481288 (Fed. Cir. Aug. 15, 2017) 11

Statutes

35 U.S.C. § 101*passim*

Other Authorities

Federal Rule of Civil Procedure 12(b)(6).....*passim*

I. INTRODUCTION

Defendant Stubhub, Inc. moves to dismiss Guyzar LLC's Complaint for Infringement of Patent (Dkt. No. 1) ("Complaint") pursuant to Rule 12(b)(6) of the Federal Rules of Civil procedure for failure to state a claim upon which relief can be granted because the asserted patent is ineligible under 35 U.S.C. § 101. The claims of the asserted '070 patent are directed to the abstract idea of confidential authentication. But authentication, like trusting a third party to certify a user, is not a technological improvement, an inventive way of applying conventional technology, or even new. Guyzar's patent does no more than withdraw a basic idea (third party confidential authentication) from the public domain without disclosing any particularized application of that idea. Therefore, the Patent-in-Suit is invalid under 35 U.S.C. § 101 for failure to claim patent-eligible subject matter.

If this Court finds that the '070 patent is not ineligible, Stubhub moves to dismiss Guyzar's Complaint because Guyzar fails to plead a plausible infringement claim. The '070 patent claims methods whose steps must all be attributable to a single party. The Complaint fails to plead how a web user's and a third party authentication provider's actions are attributable to Stubhub such that Stubhub is responsible for every step in the claimed methods. With the expiration of the '070 patent before the filing of this case, Guyzar also did not and cannot assert any form of indirect infringement. Therefore, Guyzar cannot show it is entitled to relief, and its case should be dismissed pursuant to Rule 12(b)(6).

II. NATURE AND STAGE OF PLEADINGS

On August 16, 2018, Guyzar filed this lawsuit accusing Stubhub of infringing U.S. Patent No. 5,845,070. Guyzar accuses Stubhub of infringing claim 1 by using third party sign in features on Stubhub's website. (D.I. 1 ("Compl.") ¶ 14, Fig. 3.) Stubhub has not yet answered Guyzar's complaint.

III. SUMMARY OF THE ARGUMENTS

1. Abstract ideas are ineligible for patentability under 35 U.S.C. § 101, absent an inventive

concept that amounts to significantly more than the abstract idea. The '070 patent is directed to the abstract idea of confidentially authenticating a user by relying on a third party. The '070 patent does not include an inventive concept beyond that idea. Therefore, the Court should dismiss Guyzar's Complaint pursuant to Rule 12(b)(6) for failure to state a claim.

2. Methods claims are only infringed where all the steps are attributable to a single entity. The '070 patent claims methods for a user to login to a web entity using a third party authentication service, and Guyzar's Complaint does not plead facts supporting the conclusion or inference that any third party acts are attributable to Stubhub. The Court should therefore dismiss Guyzar's Complaint pursuant to rule 12(b)(6) for failure to state a claim.

IV. STATEMENT OF THE FACTS

A. The patent-in-suit

According to Guyzar, the '070 patent, entitled "Security System for Internet Provider Transaction," allegedly discloses a confidential authentication procedure. (Compl. ¶ 14.) A user enters a "first data set," comprising at least an I.D. and password (the "first set of data"), into a "tracking and authentication control module" database holding the user's confidential information. (*See* Compl. ¶¶ 17–19.) The control module includes an "authentication server" and "certification server" for authenticating the "first data set" and validating the entity requesting a transaction, respectively. (*See* Compl. ¶ 18.) The module compares the I.D. and password to the one in the database. (*See* Compl. ¶ 19.) When the entries match, a second data set is created to be used to validate the transaction.

The '070 patent acknowledges that a number of systems for securely exchanging confidential information existed prior to its alleged December 18, 1996 priority date. '070 patent at 1:28–37. Similarly, the '070 patent acknowledges that providing data security by requiring an I.D. and password was well known prior to the alleged priority date. '070 patent at 1:45–51.

The '070 patent's three independent claims, claims 1, 7, and 13, claim substantially the same

method with only minor variations in implementation. Claim 1 is representative:

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, comprising the steps of:

accessing the Internet by the user entering a first data set into a computer based controller to control modems and communication protocols;

establishing a data base containing confidential information subject to authentication with a user's first data set;

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;

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;

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;

submitting the second data set to the certification server upon the initiation of a transaction by the user;

consummating the transaction subject to 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 data base.

According to Guyzar, these claims are practiced when a user initiates a login session on a website (such as Stubhub.com) using their third party log-in credentials (such as Facebook). (Compl. ¶ 14.) Guyzar asserts that using the OAuth standard to establish the third-party database, using said database to login the user, and issue an "Access Token" practices the claims of the '070 patent. (Compl. ¶¶ 16, 18–19.)

V. MOTION TO DISMISS PURSUANT TO 35 U.S.C. § 101.

A. This case should be decided at pleading stage under Rule 12(b)(6).

Under Federal Rule of Civil Procedure 12(b)(6), a party may move to dismiss a complaint that fails to state a claim upon which relief can be granted. The complaint survives a Rule 12(b)(6) motion if, despite “accept[ing] as true all allegations in the complaint and all reasonable inferences that can be drawn from them after construing them in the light most favorable to the nonmovant,” it fails to state a claim for relief. *Hartig Drug Co. v. Senju Pharm. Co.*, 836 F.3d 261, 268 (3d Cir. 2016) (quotations omitted). Although factual allegations are taken as true, legal conclusions are given no deference—those matters are left for the court to decide. *See Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (tenet that allegations are taken as true on a motion to dismiss “is inapplicable to legal conclusions”). “[W]hen the allegations in a complaint, however true, could not raise a claim of entitlement to relief [as a matter of law], this basic deficiency should . . . be exposed at the point of minimum expenditure of time and money by the parties and the court.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 558 (2007) (internal citations and quotations omitted). Patentability under 35 U.S.C. § 101 is a threshold legal issue. *Bilski v. Kappos*, 561 U.S. 593, 602 (2010). Accordingly, the § 101 inquiry is properly raised at the pleadings stage if it is apparent from the face of the patent that the asserted claims are not directed to eligible subject matter. *See Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 709, 718-19 (Fed. Cir. 2014) (Mayer, J., concurring). In those situations, claim construction is not required to conduct a § 101 analysis. *Genetic Techs. Ltd. v. Merial L.L.C.*, 818 F.3d 1369, 1374 (Fed. Cir. 2016) (“[C]laim construction The law of 35 U.S.C. § 101 is not an inviolable prerequisite to a validity determination under § 101.”) (brackets in original, internal citations and quotations omitted).

B. The law of 35 U.S.C. § 101.

Section 101 of the Patent Act sets forth four categories of patentable subject matter: “any new and useful process, machine, manufacture, or composition of matter.” 35 U.S.C. § 101. Also, the law recognizes three exceptions to patent eligibility: “laws of nature, physical phenomena, and abstract ideas.” *Diamond v. Chakrabarty*, 447 U.S. 303, 308 (1980) (emphasis added). Abstract ideas are ineligible

for patent protection because a monopoly over these ideas would preempt their use in all fields. *See Bilski*, 561 U.S. at 611–12. In other words, “abstract intellectual concepts are not patentable, as they are the basic tools of scientific and technological work.” *Id.* at 653 (quoting *Gottschalk v. Benson*, 409 U.S. 63, 67 (1972)).

Determining whether a patent claim is impermissibly directed to an abstract idea involves two steps. First, the court determines “whether the claims at issue are directed to a patent-ineligible concept.” *Alice*, 134 S. Ct. at 2355. Second, if the claim contains an abstract idea, the court evaluates whether there is “an ‘inventive concept’—i.e., an element or combination of elements that is sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the ineligible concept itself.” *Id.* (internal quotations and citations omitted). Transformation into a patent-eligible application requires “more than simply stating the abstract idea while adding the words ‘apply it.’” *Id.* at 2357 (quoting *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 132 S. Ct. 1289, 1294 (2012)). Indeed, if a claim could be performed in the human mind, or by a human using pen and paper, it is not patent-eligible. *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1372 (Fed. Cir. 2011). Also, a claim is not meaningfully limited if it includes only token or insignificant pre- or post-solution activity—such as identifying a relevant audience, category of use, field of use, or technological environment. *Mayo*, 132 S. Ct. at 1297-98, 1300-01.

Finally, “simply appending conventional steps, specified at a high level of generality, to laws of nature, natural phenomena, and abstract ideas cannot make those laws, phenomena, and ideas patentable.” *Mayo*, 132 S. Ct. at 1300; *see also Fort Props., Inc. v. Am. Master Lease LLC*, 671 F.3d 1317, 1323 (Fed. Cir. 2012) (“Such a broad and general limitation does not impose meaningful limits on the claim’s scope.”).

C. The '070 patent is patent-ineligible

The claims of the '070 patent are patent-ineligible because they: (1) are directed to the abstract

idea of confidentially authenticating a user; and (2) involve only conventional computer components and generic computer functions that do not, individually or in combination, make the claims patent-eligible.

For § 101 purposes, all 13 claims of the '070 patent can be evaluated collectively based on representative claim 1 because they are all “substantially similar and linked to the same abstract idea.”¹ See, e.g., *Phoenix Licensing, L.L.C. v. Consumer Cellular, Inc.*, No. 2:16-cv-152-JRG-RSP, 2017 WL 1065938, at *8-9 (E.D. Tex. Mar. 8, 2017) (invalidating 974 claims after analyzing only a few “representative claims” where the other claims were “substantially similar” and “linked to the same abstract idea.”); *Alice*, 134 S. Ct. at 2359-60 (invalidating 208 claims across four patents based on two representative claims). Regardless, as discussed below, the '070 patent claims are invalid even if considered separately and under any claim construction.

1. *Alice step one: the '070 patent is directed to an abstract idea.*

(a) Confidentially authenticating users is an abstract idea.

Stripped of its excessive verbiage, claim 1 recites the abstract idea of authenticating the identify of users by relying on a third party as a series of basic steps: (1) a database is created containing the user’s confidential data associated with login information; (2) the user enters her login information to authenticate her identity; and (3) the database issues a code authenticating the user to a third party website without disclosing the user’s confidential data. The other two independent claims claim substantially the same invention. Claim 7 adds the step of monitoring the user’s website selection and also using a third set of data for authenticating the user. Claim 13 claims substantially the same method as claim 1 from the perspective of the authorizing party. Both the specification and Guyzar’s

¹ Where claims are “substantially similar and linked to the same abstract idea,” courts may look to representative claims in a § 101 analysis. *Content Extraction and Transmission LLC v. Wells Fargo Bank, Nat’l Ass’n*, 776 F.3d 1343, 1349 (Fed. Cir. 2014).

Complaint confirm that the core of the claims—the essential, most important aspect—is the abstract idea of relying on a third party to confidentially authenticate a transaction between two others.

Authentication is an activity “humans have always performed,” *Content Extraction and Transmission LLC v. Wells Fargo Bank, Nat’l Ass’n*, 776 F.3d 1343, 1347 (Fed. Cir. 2014)—a basic tool in the “storehouse of knowledge” that is “free to all . . . and reserved exclusively to none.” *Bilski*, 561 U.S. at 602. People consummate transactions without disclosing confidential information in numerous contexts—for example, when whenever a buyer uses an agent to confidentially acquire goods or bid at auction, as recently happened with da Vinci’s *Salvator Mundi*. This basic human activity precedes the computer age. During prohibition, speakeasies required patrons to use a specific knock on the door and then provide a secret password to authenticate anyone seeking entry. A modern example is being required to show your ticket and driver’s license or passport to confirm your identity at airport security.

That the authentication methods claimed by the ’070 patent require authenticating users by a third-party and retaining the user’s confidential information does not make the claims any less abstract. Take, for example, authentication in the classic context of a spy recruiting a conspirator. The spy agency, who knows the true identity of its spy (“establishing a database”) and can recognize him (“submitting the first data set,” and “comparing the first data set”), may give the spy a code word to use when meeting a conspirator (“issuing a second data set”). To make contact, the spy could leave a note at the conspirator’s home with the code word (“submitting the second data set”). The double agent can then confirm the code word with the agency and meet the spy, without ever knowing the true identity of the spy (“consummating the transaction subject to validation of the second data set”). As this comparison illustrates, the confidential, authenticated interactions claims by the ’070 patent is no different from an activity humans have long performed—confidential, authenticated interactions—except that the claimed method is automated using conventional computer technology. *See Alice*, 134 S. Ct. at 2359 (routine activity long performed by humans and simply implemented on a computer is

not a proper basis for patentability); *Inventor Holdings, LLC v. Bed Bath & Beyond Inc.*, 123 F. Supp. 3d 557, 561 (D. Del. 2015) (finding that implementing a “longstanding commercial practice’ and a ‘method of organizing human activity’” using generic computer components did not confer eligibility).

Like other claims held ineligible, the ’070 is directed to a “fundamental economic [or] conventional business practice[.]” For example, the patent in *Inventor Holdings* was also directed to solving the problem of maintaining confidentiality of user information. 123 F. Supp. 3d at 559-560. That patent solved this problem by using a “remote and local seller” and a “code” to confirm transfer of funds. *Id.* at 561. The Court found that the claims were directed to “the abstract idea of paying for remote orders at local retailers, without reciting meaningful limitations to render the idea patent eligible.” *Id.* As here, the patent claimed the “fundamental economic [or] conventional business practice[.]” of “processing those payments without having to provide credit card information over the Internet phone, or mail.” *Id.* (quoting *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1256 (Fed. Cir. 2014)). Because “[n]one of the . . . claims [were] restricted to any specific, inventive ways of storing codes in databases or electronically applying them,” as the plaintiff argued, they were invalid. *Id.* Guyzar’s claims are directed to a similar, “fundamental business or conventional business” practice: authenticating transactions without disclosing confidential information.

(b) Because the confidential transaction is untethered to a specific implementation, it is abstract.

Even though the claimed confidential authentication methods are allegedly novel, it does not disclose any special or improved way of implementing it. To the contrary, it expressly uses well-known software and methods with conventional computer technology:

Presently available dial-up services will accept a user's personal identification number (ID) or other identifying password to bridge a proprietary communication line with Internet. Using well known point of presence (POP) the ID is submitted to an authentication server to check whether the ID is in the authentication server protocol database. Authentication will result in the POP issuing a pre-assigned framed user IP address. Thus the user is assigned a framed IP address in accordance with known systems but there is absent any control relating it to the user's Confidential

Information.

'070 patent 1:45–55. The abstract concept of the '070 patent “does not become nonabstract” merely because the claims involve the “technological environment” of conventional components and the use of standard communications systems. *Intellectual Ventures I LLC v. Symantec Corp.*, 838 F.3d 1307, 1319 (Fed. Cir. 2016) (citation omitted) (“*IV-Symantec*”); *see also Alice*, 134 S. Ct. at 2358. In *In re TLI Communications LLC Patent Litigation*, the Federal Circuit observed that although the representative claim required “concrete, tangible components such as ‘a telephone unit’ and a ‘server,’ the specification [made] clear that the recited physical components merely provide a generic environment in which to carry out the abstract idea of classifying and storing digital [data] in an organized manner.” 823 F.3d 607, 614 (Fed. Cir. 2016).

Moreover, like other computer-implemented claims found patent-ineligible, the '070 Patent claims merely claim a “desired result” without explaining “how this would be technologically implemented”—the claims specify no “particular way of programming or designing the software.” *Apple, Inc. v. Ameranth, Inc.*, 842 F.3d 1229, 1241, 1244 (Fed. Cir. 2016). Instead, they contain broad functional language and only recite a desired goal of confidentially authenticating a user without specifying any particular way to accomplish this objective. *See* '070 patent at cl. 1 (i.e., “accessing the internet,” “establishing a database,” “submitting,” “comparing,” “issuing” and “consummating the transaction . . . whereby the confidential information is retained undisclosed); *id.* at cls. 7, 13 (similar). Such “vague, functional” terms, “devoid of technical explanation as to how to implement the invention,” cannot confer eligibility. *TLI*, 823 F.3d at 615; *see also, e.g., Elec. Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350, 1356 (Fed. Cir. 2016); *Affinity Labs-DirectTV*, 838 F.3d at 1265; *Dealertrack, Inc. v. Huber*, 674 F.3d 1315, 1333 (Fed. Cir. 2012). Indeed, the widespread use of the internet for authentication and authorization, *see Ultramercial*, 772 F.3d at 716 (recognizing “ubiquitous” reach of the Internet as an information-transmitting medium), coupled with the broad scope that Guyzar

assigns to its patent claims (*see e.g.*, Compl. at ¶¶ 13–21), confirms that the claims are, at root, directed to an abstract idea. *See, e.g., Intellectual Ventures I LLC v. Capital One Bank (USA)*, 792 F.3d 1363, 1369 (Fed. Cir. 2015) (breadth confirms abstraction at *Alice* step 1) (“*IV-Capital One*”).

The ’070 patent claims are materially indistinguishable from claims directed to computer-implemented authentication and screening procedures that the Federal Circuit found were directed to abstract ideas. *Inventor Holdings* is exemplary: the Court noted that “[w]hile described as a novel alternative to traditional consumer options, the [asserted] patent describes nothing more than a retailer allowing a customer requesting goods remotely—such as via the internet or by phone—to defer payment to an in-person location.” *Inventor Holdings*, 123 F. Supp. 3d at 561. While “the concept builds upon the practice of ‘layaway’ goods” so that the customer may “keep their credit card information safe,” “[n]one of the [asserted] patent’s claims are restricted to any specific, inventive ways of storing codes in databases or electronically applying them.” *Id.* The ’070 suffers the same deficiency: the claims hypothetically claim a method that allows a user to keep their credit card information safe, but the claims are not limited to “any specific, inventive ways of storing codes in databases or electronically applying them.” *Id.* The claims here also are just as abstract as the claims for screening transactions for sufficient resources that the Supreme Court found to be abstract in *Alice*, 134 S. Ct. at 2357, and numerous other claims for analyzing information in cases such as *Electric Power*, 830 F.3d at 1352, *Content Extraction*, 776 F.3d at 1345, *FairWarning IP, LLC v. Iatric Sys., Inc.*, 839 F.3d 1089, 1092-93 (Fed. Cir. 2016), *CyberSource*, 654 F.3d at 1370 and *TLLI*, 823 F.3d at 610.

Guyzar’s allegations regarding the scope of the ’070 patent do not make the claimed invention any less abstract. In its Complaint, Guyzar alleges that the ’070 patent covers the OAuth authorization framework where a third party login is used to access a desired website. (Compl. at ¶ 14.) The specification, however, recognizes that secured authentication was known before the filing of the ’070 patent application, *see* ’070 patent at 1:45–55, and merely “[a]ppending these preexisting technologies

onto [the] claims does not make them patentable.” *Ameranth*, 842 F.3d at 1245 (using known “voice capture technologies without providing how these elements were to be technologically implemented” did not save claims at Alice step 1); *see also, e.g., IV-Symantec*, 838 F.3d at 1321-22 (claims using known virus scanning technology directed to abstract idea); *TLI*, 823 F.3d at 615 (claims “using known image compression techniques” directed to abstract idea); *Content Extraction*, 776 F.3d at 1349 (claims using “generic optical character recognition technology” directed to abstract idea).

As a result, multiple courts have found claims directed toward user authentication to be impermissibly abstract. For example, the court in *Asghari-Kamrani v. United Servs. Auto Ass’n*, 2016 WL 3670804 (E.D. Va. Jul. 5, 2016), was confronted with claims directed to similar two-step authentication features at issue in this litigation. There, the court found claims directed to “using a third party and a random, time-sensitive code to confirm the identity of a participant to a transaction” to be impermissibly abstract because they could be performed by hand or, more simply, with technologies much older than computers. *Id.* at *4. Similarly, in *OpenTV*, the court found ineligible claims “drawn to the abstract idea of using identification codes to solve [the] age-old problem” of “transmitting confidential information using unsecured communications methods.” *OpenTV, Inc. v. Apple, Inc.*, 2015 WL 1535328, at *5 (N.D. Cal. Apr. 6, 2015). The claims here merit the same treatment.

(c) Because the '070 patent claims are not directed to a specific improvement in a computer's capabilities, they are abstract.

Recent Federal Circuit cases finding claims patent-eligible at *Alice* step one are notably different from this case. *See Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327 (Fed. Cir. 2016); *McRO, Inc. v. Bandai Namco Games Am. Inc.*, 837 F.3d 1299 (Fed. Cir. 2016); *Visual Memory LLC v. NVIDIA Corp.*, 2017 WL 3481288 (Fed. Cir. Aug. 15, 2017). In those cases, unlike here, the claims recited “specific . . . improvement[s] in computer capabilities.” *Enfish*, 822 F.3d at 1336; *see also McRO*, 837 F.3d at 1313-14; *Visual Memory*, 2017 WL 3481288, at *4-5 (finding that “claims focus on a ‘specific asserted improvement in computer capabilities’—the use of programmable operational characteristics that are

configurable based on the type of processor—instead of ‘on a process that qualifies as an ‘abstract idea’ for which computers are invoked merely as a tool’”) (citation omitted).

Here, the ’070 patent “fails to provide any details for the tangible components” and “instead predominantly describes the system and methods in purely functional terms” using nothing more than conventional software routines. *See* ’070 patent at 1:45-55; 2:11-35; Fig. 1; *TLL*, 823 F.3d at 612 (distinguishing *Enfish*); *see also FairWarning*, 839 F.3d at 1094 (distinguishing *McRO* and *Enfish*). As discussed above, here the claimed steps and components “do no more than describe a desired function or outcome, without providing any limiting detail” to “confine[] the claim to a particular solution.” *Affinity Labs-DirectTV*, 838 F.3d at 1269; *see* ’070 patent at cl. 1 (reciting “accessing the internet,” “establishing a database,” and “submitting,” “issuing,” and “comparing” data); *id.* at cl. 7, 13 (similar). The ’070 patent does not purport to teach any new computer capability, but rather relies on use of the well-known capabilities of computers, as discussed. *See* ’070 patent at 1:45–55, 2:11–35.

That is, the claims of the ’070 patent do not recite “an improvement in computers as tools,” but instead “use computers as tools” to perform the abstract idea of confidentially authenticating a user by relying on a third party. *See Elec. Power*, 830 F.3d at 1354; *see also Intellectual Ventures I LLC v. J. Crew Grp., Inc.*, 2016 WL 4591794, at *6 (E.D. Tex. Aug. 24, 2016) (“[T]he ’370 Patent discloses nothing more than an abstract marketing idea implemented by general computer components.”) (citing *Enfish*, 822 F.3d at 1338). In *Enfish*, the Federal Circuit distinguished the eligible claims from others that “simply add[ed] conventional computer components to well-known business practices,” holding instead that “they [we]re drawn to a specific improvement to the way computers operate.” *Id.* at 1336. In particular, the structure of the database (according to the Federal Circuit) resulted in “increased flexibility, faster search times, and smaller memory requirements.” *Id.* at 1337. Nothing in claim 1 of the ’070 patent shows any methodology that would amount to a “specific improvement in the way computers operate.” Rather, the ’070 only claims conventional computing methods. *E.g.*, ’070

patent at cl. 1 (“establishing a database,” “comparing the user’s first data set,” and “issuing a second data set”). Therefore, the focus of the patents-in-suit is not “on [a] specific asserted improvement in computer capabilities” but instead “on a process that qualifies as an ‘abstract idea’ for which computers are invoked merely as a tool.” *Id.* at 1336.

2. *Alice step two: the '070 patent claims only implement the abstract idea of using generic computer technology, add nothing inventive, and are therefore patent-ineligible.*

The '070 patent claims fail *Alice*'s second step because they add nothing inventive to the abstract idea of confidential authentication. Each of the three independent claims (1, 7, and 13) and ten dependent claims (2–6, 8–12) merely apply the concept in particular technological environment using conventional computer components and functions. This is insufficient to make the claims patent eligible under § 101.

(a) The independent claims add nothing inventive.

Representative independent claim 1 merely recites performing the abstract idea using conventional computer functions: “accessing the Internet,” “establishing a database,” “comparing the user’s first data set,” and “issuing a second data set.” '070 patent at 21:12-36. But “accessing,” “establishing,” “submitting,” “comparing,” and “issuing” information are “basic functions of a computer” and do not make the claims eligible. *Alice*, 134 S. Ct. at 2359-60 (citation omitted). The other independent claims likewise only add “purely functional and generic” computer systems components, *id.*: “monitoring,” “providing a data base” with “a series of look up tables,” “recording the i.d. and password of the user,” “framed IP address” and “destination IP address.” '070 Patent at 21:63-22:33; 22:54-24:8. And, instead of disclosing a specific improvement to a computer or process, the '070 patent admits that the claimed authentication service is implemented using well known methods, including “point of presence (POP)” and “framed IP address[es].” *Id.* at 8:9-25 (emphasis added).

Courts have repeatedly found such components and functions to be non-inventive. In *Alice*,

for example, the Supreme Court held that claims reciting a “data processing system” with a “communications controller” for obtaining, modifying, and transmitting data was non-inventive. *Alice*, 134 S. Ct. at 2359-60. The Federal Circuit has held similar basic computer functions and components to be insufficient to confer eligibility. *See, e.g., IV-Capital One*, 792 F.3d at 1367-71 (using an “interactive interface” and “break[ing down] and organiz[ing] . . . data according to some criteria” and monitoring data is non-inventive); *buySAFE v. Google, Inc.*, 765 F.3d 1350, 1355 (Fed. Cir. 2014) (sending data over network is “not even arguably inventive”); *Dealertrack*, 674 F.3d at 1333 (“selectively forwarding” information and forwarding reply data is noninventive). And this Court has observed that “generic technological elements of the claims . . . do not transform the abstract idea into something more.” *Pragmatus Telecomms., LLC v. Genesys Telecomms. Labs., Inc.*, 114 F. Supp. 3d 192, 201 (D. Del. 2015). The same is true for the ’070 patent.

Even when these basic functions and components are viewed “as an ordered combination,” they do not reveal a “non-conventional and non-generic arrangement of known, conventional pieces” that might provide an inventive concept. *Accord Bascom Global Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341, 1350 (Fed. Cir. 2016). The claims’ arrangement of computer processes merely automate necessary steps to confidentially authenticate a user, which “cannot confer patent eligibility.” *TLI*, 823 F.3d at 615.

The independent claims’ other elements likewise add nothing inventive. Reciting a particular type of identification method (“I.D.” and “password,” as recited in claim 1, or “point of presence,” as recited in claim 7) is a classic field-of-use limitation that is “not even arguably inventive.” *Id.* at 614 (citation omitted). Moreover, the use of digital identification and point of presence to identify internet users was well-known at the time of the purported invention, as the ’070 patent acknowledges. *See* ’070 patent at 1:1:45–51. As this Court has recognized, “[a] claim that recites an abstract idea must include additional features” that must be more than “the recitation of a generic computer.” *Pragmatus*

Telecom, 114 F. Supp. 3d at 198 (citations omitted); *see also Elec. Power*, 830 F.3d at 1355 (“off-the-shelf, conventional computer, network . . . technology for gathering, sending, and presenting the desired information” is insufficient); *IV-Symantec*, 838 F.3d at 1319; *Content Extraction*, 776 F.3d at 1348. The independent claims here add nothing beyond unspecified conventional computer components implemented with a well known software to merely perform the abstract idea.

Unlike the handful of particular enhancements to computer technology (or application of the abstract idea to improve another technology or process) that the Federal Circuit has found eligible at *Alice* step two, the claims here merely apply an “old solution” (two-factor authentication) in a computer environment without specifying how it is accomplished. *See Synopsis, Inc. v. Mentor Graphics Corp.*, 839 F.3d 1138, 1151-52 (Fed. Cir. 2016) (distinguishing *DDR Holdings*, 773 F.3d at 1256 and *Bascom*). Thus, the independent claims add only insignificant limitations that do not render those claims patent eligible.

(b) The dependent claims add nothing inventive.

The additional limitations in the dependent claims do not confer patent-eligibility because they recite either token post-solution limitations or elements performed by computing elements that are “purely conventional,” merely requiring “a generic computer to perform generic computer functions.” *Alice*, 134 S. Ct. at 2359. Specifically:

- Claim 2 specifies using a framed IP address for the second data set;
- Claim 3 requires confirming the framed IP address and certifying the user’s credit;
- Claim 4 requires that the user inputs the second data set to the Internet Entity and the Internet Entity verifies the second data with the certifications server;
- Claims 5 and 6 provides that the data base comprises look up tables and are updated in real time;
- Claim 8 specifies that the third data set is the destination address of the internet entity;
- Claim 9 recites that the computer “based controller” is a point of presence program;
- Claim 10 provides that the certificate server also authorizes the internet entity to conduct transactions;
- Claim 11 specifies that the third data set is used to track which internet entity is browsed by the user; and

- Claim 12 adds using the certification module to bill charges to the user.

These trivial limitations cannot confer patent eligibility. *See, e.g., Bilski*, 561 U.S. at 612 (“limiting an abstract idea to one field of use or adding token post-solution components d[oes] not make the concept patentable”). For example, claim 2 merely expands on the data set limitation recited in claim 1, but the addition of this conventional computer function fails to add anything inventive to the otherwise patent-ineligible concept. Other claims merely specify a preferred method of data storage and tracking (claims 5, 6, 8, and 11), require certification of more data (claims 3, 4, 10 and 12), or require a “well known” internet interface method (claim 9). These are conventional activities that can take place during any authentication procedure. Simply reciting particular types of information, policies, or constraints does not make the claims eligible, just as it added nothing inventive to recite particular media content (“text data, music data, [or] video data”) in *Ultramercial*, 772 F.3d at 712, particular “sources” and “types” of data in *Electric Power*, 830 F.3d at 1355, or a particular type of information to be selectively forwarded in *Dealertrack*, 674 F.3d at 1333. Claim 13’s requirement that the authentication service “transmit” information is also abstract because it could be performed with technologies much older than computers (e.g., by hand). *See Asghari-Kamrani*, 2016 WL 3670804 at *4. These dependent claims are thus also patent-ineligible under § 101.

(c) The ’070 patent claims are patent-ineligible under any claim constructions.

The § 101 issue can be resolved without claim construction because the routine steps of “accessing the internet,” “establishing a database,” “submitting” and “comparing” data, “issuing” and “submitting” more data, and “consummating the transaction” (’070 Patent at cl. 1) can be well understood without construction. *O2 Micro Intl. Ltd. v. Beyond Innovation Tech. Co.*, 521 F.3d 1351, 1360-63 (Fed. Cir. 2008) (emphasizing that claim construction is not an obligatory exercise in redundancy and is not required when terms have a well-understood meaning); *see also Ultramercial*, 772 F.3d at 714-15 (declining to require claim construction prior to dismissal under § 101 where the claims practiced

an abstract idea through routine steps). The claimed steps are so generic (e.g., “accessing,” “establishing,” “submitting” “issuing” and “comparing”), and the implementation so conventional (e.g., “a method of [authenticating/controlling] a user’s confidential information . . . for conducting internet transactions”), that no construction would provide meaningful limitations to transform the abstract nature of the claims into an otherwise eligible and inventive concept. *See* ’070 patent at cls. 1, 7, 13; *Alice*, 134 S. Ct. at 2357.

VI. MOTION TO DISMISS FOR FAILURE TO STATE A CLAIM

A. The law of Rule 12(b)(6).

Allegations of joint infringement are held to the *Iqbal* and *Twombly* standard. *See Lyda v. CBS Corp.*, 838 F.3d 1331, 1339 (Fed. Cir. 2016). A plaintiff must provide the grounds of his entitlement to relief, and must allege specific facts in support of each such claim, sufficient to “state a claim to relief that is plausible on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 547 (2007). “[A] plaintiff’s obligation to provide the ‘grounds’ of his ‘entitle[ment] to relief’ requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do.” *Id.* at 555. “Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). To survive a Rule 12(b)(6) motion, a plaintiff must “plausibly allege that Defendant[] exercise[d] the requisite ‘direction or control’ over the performance of the claim steps, such that performance of every step is attributable to Defendant[].” *Lyda*, 838 F.3d at 1340. A bare assertion that the defendant controls other entities, without any factual allegations relating to how the defendant exercises such control, cannot form the basis of a reasonable inference that each element of any claim is attributable to the defendant. *See id.* (holding that alleging direction or control “conclusively and without factual support” failed “to plausibly plead sufficient facts to ground a joint infringement claim”).

B. Guyzar has not pleaded sufficient detail to provide notice of its joint infringement allegations.

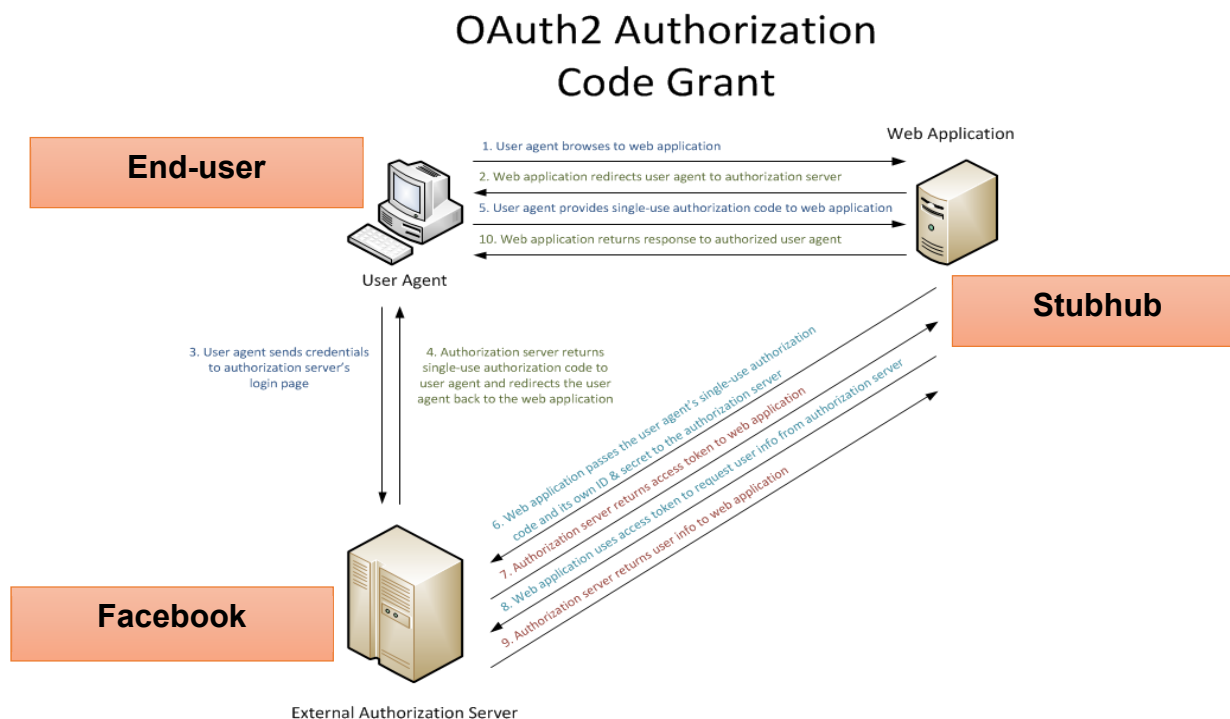
Guyzar's pleadings do not support plausible infringement claim against Stubhub. The Complaint concedes that *three* parties are involved in the accused OAuth authentication standard method: Stubhub as the provider of its website (Complaint ¶ 14), an end-user of the website (*id.* ¶¶ 22–24), and a third party running an authentication server, such as Facebook (*id.* ¶ 23 (“in combination with Facebook”)).

Guyzar is attempting to plead joint infringement, which does not automatically lead to a plausible claim of infringement by Stubhub. “Where more than one actor is involved in practicing the steps [of a method claim], a court must determine whether the acts of one are attributable to the other such that a single entity is responsible for the infringement. [The law] will hold an entity responsible for others’ performance of method steps in two sets of circumstances: (1) where that entity directs or controls others’ performance, and (2) where the actors form a joint enterprise.” *Akamai Techs., Inc. v. Limelight Networks, Inc.*, 797 F.3d 1020, 1022 (Fed. Cir. 2015). Here, joint infringement requires the complaint to support a reasonable inference that all method steps are performed, and either: (1) Stubhub exercises the requisite “direction or control” over the others’ performance; or (2) all actors form a joint enterprise such that performance of every step is attributable to the controlling party. *Lyda*, 838 F.3d at 1339. Guyzar has not pleaded facts showing that Stubhub directs or controls Facebook, or that Stubhub, the end-user, and Facebook form a joint enterprise.

First, Guyzar’s Complaint fails to explain which of the end-user, Stubhub, or a third party such as Facebook performs each step of the asserted claims. Instead, Guyzar’s Complaint only comprises general assertions that the *accused instrumentality* uses an industry standard login and authentication standard to provide the claimed method, without describing how each party participates. (Compl. ¶ 14.) As explained below, the accused instrumentality necessarily involves three parties, and Guyzar must plead which party performs which claim steps and allege facts sufficient to

attribute liability for such performance to Stubhub. It has not done so.

Second, even had Guyzar identified which party performs each claim limitation, it is clear that a third party, such as Facebook, is necessarily one of those parties. The accused OAuth standard is a framework that “enables a *third-party application* to obtain limited access to an HTTP service.” See OAuth 2.0 Authorization Framework available at <https://tools.ietf.org/html/rfc6749> (last accessed September 10, 2018).² An exemplary implementation of the standard’s framework is illustrated and annotated below, identifying the three parties allegedly involved with the accused instrumentality:



See <https://stackoverflow.com/questions/28487586/owin-oauth2-3rd-party-login-authentication-from-client-app-authorization-from> (last accessed September 4, 2018) (annotated).

The best plausible reading of the Complaint is that several steps of the claimed invention are

² The Court may consider documents attached to a motion to dismiss if they are referred to in the complaint and are central to the plaintiff’s claim. *Gines v. D.R. Horton, Inc.*, 699 F.3d 812, 820 (5th Cir. 2012); *Collins v. Morgan Stanley Dean Witter*, 224 F.3d 496, 498-99 (5th Cir. 2000) (citing *Venture Assocs. Corp. v. Zenith Data Sys. Corp.*, 987 F.2d 429, 431 (7th Cir. 1993)).

necessarily performed by two third parties: Facebook, which retains the user's login/password information and other confidential information and provides the external authentication server, and the end user, which enters those credentials into the computer. The Complaint identifies this information as "third-party log-in credentials." (Compl. Fig. 3.) It first alleges that the end-user performs the step of entering these credentials to meet the first element of Claim 1. It then alleges that maintaining and authenticating these credentials—a step that would allegedly be performed by Facebook—meets the second step of Claim 1. (*Id.* ¶¶ 15–16.) After the user successfully logs into Facebook with these credentials, Facebook's authorization server provides an authentication token to Stubhub, which the Complaint alleges meets at least elements three, four, and five of Claim 1. (*Id.* ¶¶ 17–19.)

Because the Complaint alleges that the *end-user* performs the first element, it attempts to plead elements of direction or control of the end-user to try to establish joint infringement. (*Id.* ¶¶ 23–24). The Complaint, however, also concedes that the accused OAuth standard must be performed "in combination with Facebook," *id.* ¶ 23, but it does not allege any facts that demonstrate that Stubhub directs or controls Facebook's performance of these steps. Nor does it plead that Facebook and Stubhub have entered into a joint enterprise. Such an allegation would be frivolous anyway.

Thus, Guyzar fails to "state a claim to relief that is plausible on its face." As demonstrated above, any such allegation would be frivolous, and amending the Complaint to add the missing allegations would be futile. *Twombly*, 550 U.S. at 547.

VII. CONCLUSION

For the foregoing reasons, Stubhub respectfully requests that the Court dismiss Guyzar's Complaint for failure to state a claim upon which relief can be granted. Because leave to amend would be futile, Stubhub requests dismissal with prejudice.

Dated: September 10, 2018

Respectfully submitted,

FISH & RICHARDSON P.C.

By: /s/ Jeremy D. Anderson
Jeremy D. Anderson (#4515)
222 Delaware Ave., 17th Floor
P.O. Box 1114
Wilmington, DE 19801
(302) 652-5070 (Telephone)
(302) 652-0607 (Facsimile)
janderson@fr.com

Neil J. McNabnayd
William B. Collier
1717 Main Street, Suite 5000
Dallas, TX 75201
(214) 747-5070 (Telephone)
(214) 747-2091 (Facsimile)
mcnabnay@fr.com
collier@fr.com

**COUNSEL FOR DEFENDANT
STUBHUB, INC.**