

1 HILL, KERTSCHER & WHARTON, LLP

2 Vivek Ganti (SBN 275554)

3 Steven G. Hill (*pro hac vice* pending)

3350 Riverwood Parkway, Suite 800

4 Atlanta, GA 30339

5 Telephone: (770) 953-0995

6 Fax: (770) 953-1358

E-Mail: VG@hkw-law.com

SGH@hkw-law.com

7 VICK LAW GROUP, APC

8 Scott Vick (SBN 171944)

9 800 West Sixth Street, Suite 1220

10 Los Angeles, California 90017

11 Telephone: (213) 784-6225

12 Facsimile: (213) 784-6227

E-mail: Scott@vicklawgroup.com

13 *Attorneys for Plaintiff Computer Protection*  
14 *IP, LLC*

15 **UNITED STATES DISTRICT COURT**  
16 **CENTRAL DISTRICT OF CALIFORNIA**

17 COMPUTER PROTECTION IP,  
18 LLC

Plaintiff,

19 vs.

20 DREAMHOST, LLC., and NEW  
21 DREAM NETWORK, LLC.

Defendants.

Case No. 2:17-CV-08858 JAK (JEMx)

**SECOND AMENDED  
COMPLAINT FOR PATENT  
INFRINGEMENT**

**JURY TRIAL DEMANDED**

Computer Protection IP, LLC. (“Computer Protection” or “Plaintiff”) files this Second Amended Complaint against DreamHost, LLC and New Dream Network, LLC (collectively, “DreamHost” or “Defendant”) for infringement of U.S. Patent. No. 8,468,591 (“the ’591 Patent” or the “Patent-in-Suit”), hereby alleging as follows:

### **Nature of the Suit**

1. This is a claim for patent infringement arising under the patent laws of the United States, Title 35 of the United States Code. This is a civil action for the infringement of the ’591 Patent (attached hereto as Exhibit “A”) against DreamHost under the Patent Laws of the United States 35 U.S.C. § 1, *et seq.*

### **The Parties**

2. Computer Protection is a Georgia limited liability company.

3. Computer Protection owns the Patent-in-Suit.

4. DreamHost, LLC is a Delaware limited liability web hosting and computer services company business authorized to do business in California and having its principal place of business at 707 Wilshire Blvd., Suite 5050, Los Angeles, CA 90017. DreamHost, LLC is owned and operated by New Dream Network, LLC, a California limited liability company having a principal place of business in this District, located at 707 Wilshire Blvd., Suite 5050, Los Angeles, California 90017. DreamHost can be served with process by service upon its registered agent CT Corporation System, 818 West Seventh Street, Suite 930, Los Angeles, CA 90017.

5. As shown in this Complaint, DreamHost makes and uses a cloud-based operating system called the “DreamHost Cloud,” which controls large pools of computer, storage, and networking resources throughout a datacenter, managed through a dashboard that gives administrators control while empowering their users to provision resources through a web interface. As explained herein, at a

1 minimum, the making and use of said system by DreamHost directly infringes the  
2 Patent-in-Suit.

### 3 **Jurisdiction and Venue**

4 6. This Court has jurisdiction over the subject matter of this action  
5 pursuant to 28 U.S.C. §§ 1331 and 1338(a) because this action arises under the  
6 patent laws of the United States, including 35 U.S.C. § 271 *et seq.*

7 7. Venue is proper in this judicial District pursuant to 28 U.S.C. §§ 1391  
8 and 1400(b). Among other things, DreamHost resides and transacts business in  
9 this District. Furthermore, on information and belief, DreamHost has committed  
10 acts of patent infringement in this District, including the making and use of the  
11 system described in paragraph 5 above.

12 8. On information and belief, DreamHost is subject to this Court's  
13 specific personal jurisdiction pursuant to due process, due at least to its substantial  
14 business in this forum, including (i) at least a portion of the infringements alleged  
15 herein; and (ii) regularly doing or soliciting business, engaging in other persistent  
16 courses of conduct, and/or deriving substantial revenue from goods and services  
17 provided to individuals in California and in this District.

### 18 **The '591 Patent**

19 9. The '591 Patent, titled "Client Authentication and Data Management  
20 System," was duly and legally issued by the United States Patent and Trademark  
21 Office on June 18, 2013. *See* Ex. A. Ariel Silverstone is the inventor of the '591  
22 Patent.

23 10. Enterprise-wide computer systems are being accessed more than ever  
24 via a variety of computing devices which are difficult to track. This is a problem  
25 unique in the field of computing. Unauthorized access into computer systems  
26 compromises and even undermines the efficiency of these systems.  
27  
28

1           11. When remote unauthorized access to a computer system occurs, it  
2 may or may not be detected in time to prevent the attacker from accessing sensitive  
3 data, destroying sensitive data, or implanting bogus data into the network.

4           12. Prompt responses to successful security breaches often include the use  
5 of security automation tools, in order to limit the amount of time an attacker has  
6 access to the network. These tools, however, consume valuable computer  
7 resources and reduce the overall efficiency of the computer network.

8           13. These security automation tools include intrusion prevention systems  
9 (IPS). When an IPS detects a potential incursion, it will automatically block  
10 network traffic, preventing attacks from reaching their intended targets. IPS  
11 systems at work consume valuable computer resources and reduce the overall  
12 efficiency of the computer network.

13           14. If an unwanted intrusion into a computer system occurs, data loss  
14 prevention (DLP) systems may also step in and seek to prevent the successful theft  
15 of sensitive information. DLP systems at work consume valuable system resources  
16 and reduce the overall efficiency of the computer network. DLP systems monitor  
17 traffic leaving the network, looking for transmissions of sensitive information by  
18 system users. If the DLP solution detects such activity, it can notify security  
19 administrators.

20           15. In the wake of a detected, unauthorized access into a computer  
21 system, security analysts responding will often perform a manual investigation into  
22 the breach, looking for evidence of how the attacker gained access and using that  
23 information to stop the flow of data out of the organization. Actions taken by  
24 security professionals may include changing firewall rules, updating security  
25 policies, adding hosts to a blacklist and quarantining suspect systems. These  
26 actions require security analysts to consume valuable computer resources and  
27 reduce the overall efficiency of the computer network in the near term.  
28

1           16. Automated forensic tools also allow the close examination of systems  
2 involved after an unauthorized access event has occurred. Security information and  
3 event management (SIEM) systems allow the review and correlation of records  
4 from a wide variety of technology components, as well as threat intelligence  
5 information from security partners. The use of these systems, however, consume  
6 valuable computer resources and reduce the overall efficiency of the computer  
7 network.

8           17. The Internet of things (“IoT”) is the network of physical devices,  
9 vehicles, home appliances and other items embedded with electronics, software,  
10 sensors, actuators, and connectivity which enables these objects to connect and  
11 exchange data. The increasing trend towards IoT has only exacerbated concerns  
12 about how access by unauthorized devices may compromise the efficient operation  
13 of the IoT.

14           18. IoT includes a collection of objects equipped with sensors which  
15 generate data and transmit it over a communications network to each other and to  
16 servers which control the sensors and collect data from them.

17           19. An example of this is a smart metering system, which involves a  
18 network of electricity meters that measure consumer electricity usage and send the  
19 data back to an electricity company's servers. The servers may also send data, such  
20 as tariff changes or firmware updates, back to the meters.

21           20. In the example above, a fake meter that transmits false data (probably  
22 indicating less consumption than is actually occurring) could be installed on the  
23 network to impersonate a genuine one.

24           21. In other example, malicious users could install a fake server to issue  
25 malicious commands or upload malicious firmware to meters on the network.

26           22. In another example, injecting fake measurements upon unauthorized  
27 access could disrupt the control processes and cause them to react inappropriately  
28 or dangerously, or could be used to mask physical attacks.

1           23. In another example, sending incorrect commands could be used to  
2 trigger unplanned events, to deliberately send some physical resource (water, oil,  
3 electricity, etc.) to an unplanned destination.

4           24. These examples are meant to illustrate the potentially devastating  
5 impacts that unauthorized access poses to the efficiency and efficient operation of  
6 the IoT and underlying computer systems used to support it.

7           25. Recognizing that enterprise-wide computer systems are now being  
8 accessed more than ever via a variety of computing devices which are difficult to  
9 track, numerous solutions have been proposed and adopted. For example, Network  
10 Access Control (NAC) is an approach that attempts to unify endpoint security  
11 technology user or system authentication and network security enforcement. Other  
12 approaches include the adoption of public key cryptography standards.

13           26. The '591 Patent identifies a new approach to solve this technological  
14 problem. Generally speaking, it improves the security of these systems by special  
15 programming and a unique tool in the field of computing, i.e., a thin layer of  
16 virtual machine management software, configured to create a virtual machine  
17 manager which will assume control over system access during the boot process.  
18 The claims of the '591 Patent describe implementing a unique virtual machine  
19 manager which is configured specially to operate in conjunction with the  
20 authentication server of an enterprise computer system to implement an  
21 authentication process that in turn controls the boot process as a means of  
22 protecting a system against access by an unauthorized computing device. The  
23 claims of the '591 Patent, which were invented in 2006, achieve this solution using  
24 a non-conventional and non-generic arrangement of computing components.

25           27. The claims of the '591 Patent include an arrangement of computing  
26 components which were not routine, conventional or generic in or before the 2006  
27 time frame. Specifically, in and before 2006, virtualization technologies were not  
28 referred to or used in communication with an authentication server. Attached as

1 Exhibit B is a June 26, 2006 article from IT Pro on virtualization technologies  
2 which is representative of the state of the art at that time. The articles provides a  
3 thorough discussion of the use of virtual machines with desktops and servers,  
4 including a detailed discussion of the state of the product offerings and solutions in  
5 the virtualization space. None of the technologies in question relate to playing a  
6 part in the authentication of protected computing devices.

7 28. Attached as Exhibit C is an “Overview of Authentication and  
8 Authorization Technologies and Solution End States” published by Microsoft and  
9 dated June 27, 2006. It provides a thorough overview of authentication and  
10 authorization technologies surrounding user access to operating systems such as  
11 Microsoft Windows®. In the discussion provided by the article, there is no  
12 reference to the use of a hypervisor or any other virtual machine manager.

13 29. Based at least upon the foregoing, and the teachings of other similar  
14 references in and before 2006, the limitations in each of the claims of the ‘591  
15 Patent relating to the reconfiguration of a standard virtual machine manager into a  
16 specially programmed used to communicate with an authentication server during  
17 the boot process was not common, routine, ordinary, well-understood,  
18 conventional or generic at the time of invention.

19 30. Computer Protection is the exclusive owner of all rights, title, and  
20 interest in the ‘591 Patent and has the right to sue and recover for any past, current  
21 or future infringement of the ‘591 Patent.

22 31. The ‘591 Patent is valid and enforceable.

### 23 **The DreamHost Cloud and DreamCompute**

24 32. As described herein, DreamHost makes and uses the DreamHost  
25 Cloud, a cloud-based system that provides centralized network control of data  
26 processing resources including storage and servers hosted on networked computing  
27 devices. This cloud-based operating system controls large pools of compute,  
28 storage, and networking resources, all managed through a dashboard that gives

1 administrators control while empowering their users to provision resources through  
2 a web interface. DreamHost Cloud is used by DreamHost to control cloud  
3 computing environments providing Infrastructure as a Service (IaaS) and Platform  
4 as a Service (PaaS) capabilities. These capabilities require coordination and control  
5 of distributed computing resources including compute nodes and storage nodes  
6 interconnected by and communicating over a high-speed computer network.

7 33. DreamHost's first product built on the architecture and resources of  
8 the aforementioned DreamHost Cloud system is DreamCompute. DreamCompute  
9 allows customers to create virtual machines, block devices, and networks on-  
10 demand via standard APIs and command-line tools or via an intuitive web-based  
11 user interface. DreamHost offers the use of DreamCompute to its customers for a  
12 fee.

13 34. DreamCompute runs on a mixture of high-end Dell servers running  
14 Ubuntu Linux.

15 35. Server types being used to support DreamCompute include storage  
16 nodes and hypervisor nodes for hosting and managing virtual machines (VMs).  
17 These are the server types generally used to support the DreamHost Cloud system.

18 36. The DreamCompute hypervisor nodes are optimized for hosting VMs  
19 running on top of a KVM hypervisor, featuring 64 AMD cores and 192 GB of  
20 RAM.

21 37. The DreamCompute VMs are started by creating an instance using the  
22 DreamCompute dashboard.

23 38. In DreamCompute, each instance is based on a flavor. Flavors define  
24 the amount of resources allocated to the VM in terms of vCPUs, memory, and boot  
25 volume size.

26 39. DreamCompute provides Flavors small enough for companies just  
27 starting out to large ones for companies with greater computing needs.  
28

1           40. The storage nodes in DreamCompute are lower-powered, higher-  
2 density servers, each with twelve 3 TB disks, each running Ceph, which is an open  
3 source, massively distributed, fault tolerant storage system.

4           41. As is the case with DreamHost Cloud, DreamCompute features a  
5 “cockpit” pod, which represents the “brain” of the cloud.

6           42. In the aforementioned cockpit pod, services run on a mixture of bare  
7 metal and VMs, including Horizon, Glance, Nova, Neutron, Keystone, and Cinder,  
8 along with Apache, HAProxy load balancers, MySQL databases, and RabbitMQ  
9 queueing systems. The entire system is configured and managed by Chef, and is  
10 monitored using open source tools (*e.g.*, logstash, graphite, collectd, and nagios).

11           43. Every VM in DreamCompute boots from a virtual block device  
12 backed by a multi-petabyte Ceph storage cluster. Operating system images  
13 themselves are stored in the same cluster as these block devices, enabling  
14 DreamCompute to leverage Ceph’s Copy-on-Write (COW) functionality. Rather  
15 than downloading the operating system image from a central store to a hypervisor  
16 (which is time consuming) and then provisioning a new block device, Ceph  
17 enables the VMs to boot nearly instantly from a thin-provisioned copy of the OS  
18 image. As a result, VMs in DreamCompute can be created and fully operational in  
19 as little as 40 seconds.

20           44. DreamCompute was built to provide full network virtualization for  
21 every customer. In DreamCompute, the physical network represents an “underlay,”  
22 which is invisible to the customer. A virtual network fabric – an “overlay” – is then  
23 layered on top, providing every customer in DreamCompute with a virtual OSI  
24 Layer 2 (L2) switch, which is completely isolated at L2 from every other customer.

#### 25           **COUNT I – INFRINGEMENT OF THE ‘591 PATENT**

26           45. Plaintiff incorporates by reference the preceding paragraphs 1-27 as if  
27 they were restated fully herein.  
28

1           46. On February 21, 2018, Plaintiff served upon counsel for the  
2 Defendants its Preliminary Infringement Contentions. A true and correct copy of  
3 these contentions are attached as Exhibit D. Plaintiff asserts that claims 1, 3, 4, 6,  
4 8, 13, 17, 39, 40, 41, 42, 43, 48, 49 and 52 (“Asserted Claims”) are infringed by  
5 the DreamHost Cloud and DreamHost Compute (“Accused Instrumentalities”).  
6 *See* Ex. D, p. 2.

7  
8           47. Each of the limitations of claim 1 of the ’591 Patent are embodied in  
9 the making and in the use of DreamHost Cloud and in the related DreamCompute  
10 product. As such, DreamHost Cloud and DreamCompute infringe claim 1 of the  
11 ’591 Patent. *See* Ex. D, pp. 4-23 (Claim Chart providing infringement analysis of  
12 claim 1).

13           48. Each of the limitations of claim 3 of the ’591 Patent are embodied in  
14 the making and in the use of DreamHost Cloud and in the related DreamCompute  
15 product. As such, DreamHost Cloud and DreamCompute infringe claim 1 of the  
16 ’591 Patent. *See* Ex. D, pp. 23-24 (Claim Chart providing infringement analysis of  
17 claim 1).

18           49. Each of the limitations of claim 4 of the ’591 Patent are embodied in  
19 the making and in the use of DreamHost Cloud and in the related DreamCompute  
20 product. As such, DreamHost Cloud and DreamCompute infringe claim 1 of the  
21 ’591 Patent. *See* Ex. D, pp. 24-25 (Claim Chart providing infringement analysis of  
22 claim 1).

23           50. Each of the limitations of claim 6 of the ’591 Patent are embodied in  
24 the making and in the use of DreamHost Cloud and in the related DreamCompute  
25 product. As such, DreamHost Cloud and DreamCompute infringe claim 1 of the  
26 ’591 Patent. *See* Ex. D, pp. 25-26 (Claim Chart providing infringement analysis of  
27 claim 1).  
28

1           51. Each of the limitations of claim 8 of the '591 Patent are embodied in  
2 the making and in the use of DreamHost Cloud and in the related DreamCompute  
3 product. As such, DreamHost Cloud and DreamCompute infringe claim 1 of the  
4 '591 Patent. *See* Ex. D, pp. 26-27 (Claim Chart providing infringement analysis of  
5 claim 1).

6           52. Each of the limitations of claim 13 of the '591 Patent are embodied in  
7 the making and in the use of DreamHost Cloud and in the related DreamCompute  
8 product. As such, DreamHost Cloud and DreamCompute infringe claim 1 of the  
9 '591 Patent. *See* Ex. D, pp. 27-28 (Claim Chart providing infringement analysis of  
10 claim 1).

11           53. Each of the limitations of claim 17 of the '591 Patent are embodied in  
12 the making and in the use of DreamHost Cloud and in the related DreamCompute  
13 product. As such, DreamHost Cloud and DreamCompute infringe claim 17 of the  
14 '591 Patent. *See* Ex. D, pp. 28-29 (Claim Chart providing infringement analysis of  
15 claim 1).

16           54. Each of the limitations of claim 39 of the '591 Patent are embodied in  
17 the making and in the use of DreamHost Cloud and in the related DreamCompute  
18 product. As such, DreamHost Cloud and DreamCompute infringe claim 1 of the  
19 '591 Patent. *See* Ex. D, pp. 29-34 (Claim Chart providing infringement analysis of  
20 claim 1).

21           55. Each of the limitations of claim 40 of the '591 Patent are embodied in  
22 the making and in the use of DreamHost Cloud and in the related DreamCompute  
23 product. As such, DreamHost Cloud and DreamCompute infringe claim 1 of the  
24 '591 Patent. *See* Ex. D, pp. 34-35 (Claim Chart providing infringement analysis of  
25 claim 1).

26           56. Each of the limitations of claim 41 of the '591 Patent are embodied in  
27 the making and in the use of DreamHost Cloud and in the related DreamCompute  
28 product. As such, DreamHost Cloud and DreamCompute infringe claim 1 of the

1 '591 Patent. *See* Ex. D, pp. 35-36 (Claim Chart providing infringement analysis of  
2 claim 1).

3 57. Each of the limitations of claim 42 of the '591 Patent are embodied in  
4 the making and in the use of DreamHost Cloud and in the related DreamCompute  
5 product. As such, DreamHost Cloud and DreamCompute infringe claim 1 of the  
6 '591 Patent. *See* Ex. D, p. 36. (Claim Chart providing infringement analysis of  
7 claim 1).

8 58. Each of the limitations of claim 43 of the '591 Patent are embodied in  
9 the making and in the use of DreamHost Cloud and in the related DreamCompute  
10 product. As such, DreamHost Cloud and DreamCompute infringe claim 1 of the  
11 '591 Patent. *See* Ex. D, p. 36 (Claim Chart providing infringement analysis of  
12 claim 1).

13 59. Each of the limitations of claim 48 of the '591 Patent are embodied in  
14 the making and in the use of DreamHost Cloud and in the related DreamCompute  
15 product. As such, DreamHost Cloud and DreamCompute infringe claim 1 of the  
16 '591 Patent. *See* Ex. D, pp. 37-44 (Claim Chart providing infringement analysis of  
17 claim 1).

18 60. Each of the limitations of claim 49 of the '591 Patent are embodied in  
19 the making and in the use of DreamHost Cloud and in the related DreamCompute  
20 product. As such, DreamHost Cloud and DreamCompute infringe claim 1 of the  
21 '591 Patent. *See* Ex. D, pp. 44-45 (Claim Chart providing infringement analysis of  
22 claim 1).

23 61. Each of the limitations of claim 52 of the '591 Patent are embodied in  
24 the making and in the use of DreamHost Cloud and in the related DreamCompute  
25 product. As such, DreamHost Cloud and DreamCompute infringe claim 1 of the  
26 '591 Patent. *See* Ex. D, pp. 45-46 (Claim Chart providing infringement analysis of  
27 claim 1).

28 62.

1           63. DreamHost makes and uses the DreamHost Cloud system, which  
2 literally infringes at least one claim of the '591 Patent under 35 U.S.C. § 271(a).

3           64. Specifically, DreamHost infringes at least one claim of the '591  
4 Patent by testing, developing, designing, validating, or otherwise making or using  
5 the DreamHost Cloud system, or similar versions thereof, for development,  
6 marketing, training, or commercial purposes.

7           65. DreamHost also makes, uses, offers for sale and sells DreamCompute  
8 to its customers. DreamCompute infringes at least one claim of the '591 Patent  
9 under 35 U.S.C. § 271(a).

10           66. Specifically, DreamHost infringes at least one claim of the '591  
11 Patent by testing, developing, designing, validating, or otherwise making, using,  
12 offering for sale, or selling DreamCompute, or similar versions thereof, for  
13 development, marketing, training, or commercial purposes.

14           67. Third parties, including the DreamHost customers, have infringed,  
15 and continue to infringe, one or more claims of the '591 Patent under 35 U.S.C. §  
16 271(a), either literally and/or under the doctrine of equivalents, by using  
17 DreamCompute in the United States.

18           68. Through its actions relating to the marketing, offer for sale and sale of  
19 DreamCompute, and making and use of the DreamHost Cloud to support  
20 DreamCompute, DreamHost has encouraged and caused its customers to infringe  
21 one or more claims of the '591 Patent. DreamHost knew or should have known  
22 that its acts would cause its customers to infringe the '591 Patent, in this District  
23 and elsewhere in the United States.

24           69. DreamHost has knowledge and notice of the '591 Patent and its  
25 infringement as of the date of the service of the original complaint in this case.

26           70. Nevertheless, DreamHost has induced infringement, and continues to  
27 induce infringement, of one or more claims of the '591 Patent under 35 U.S.C. §  
28 271(b). DreamHost actively, knowingly, and intentionally induced, and continues

1 to actively, knowingly, and intentionally induce, infringement of the '591 Patent  
2 by marketing, selling and supporting DreamCompute with the knowledge and  
3 intent that third parties will use DreamCompute in the United States, for its  
4 intended purpose, which infringes the '591 Patent; and with the knowledge and  
5 intent to encourage and facilitate the infringement through the dissemination of  
6 DreamCompute and/or the creation and dissemination of documentation and  
7 technical information related to DreamCompute.

8 71. Computer Protection is currently the exclusive owner of all rights,  
9 title, and interest in the '591 Patent and has the right to sue and recover for any  
10 damages caused by past infringement of the '591 Patent, including the damages  
11 DreamHost's infringement has caused to Computer Protection.

12 72. Computer Protection has been and continues to be damaged by  
13 DreamHost's infringement of the '591 Patent. As such, Computer Protection is  
14 entitled to an award of money damages. This includes, but is not limited to, a  
15 reasonable royalty.

16 73. Upon information and belief, DreamHost will continue to infringe the  
17 '591 Patent unless enjoined by this Court.

18 **Prayer for Relief**

19 Wherefore, Plaintiff Computer Protection respectfully requests that this  
20 Court enter judgment as follows:

- 21 a) adjudging that one or more the claims of the '591 Patent are valid and  
22 infringed, either literally and/or under the doctrine of equivalents;  
23 b) awarding Computer Protection all damages to which it is entitled  
24 under 35 U.S.C. § 284, including but not limited to a reasonable  
25 royalty, for the past infringement and any continuing or future  
26 infringement, and ordering a full accounting of the same;  
27 c) awarding Computer Protection pre-judgment and post-judgment  
28 interest on its damages; and

1 d) awarding Computer Protection such other and further relief in law or  
2 equity that the Court deems just and proper.  
3

4 Dated: March 7, 2018

VICK LAW GROUP, APC

5 By: /s/ Scott Vick

6 Scott Vick (SBN 171944)

7 Scott@vicklawgroup.com

8 800 West Sixth Street, Suite 1220

9 Los Angeles, California 90017

10 Telephone: (213) 784-6225

11 Facsimile: (213) 784-6227

12 Vivek Ganti (SBN 275554)

13 Steven G. Hill (*pro hac vice* pending)

14 VG@hkw-law.com

15 SGH@hkw-law.com

16 HILL, KERTSCHER & WHARTON, LLP

17 3350 Riverwood Parkway, Suite 800

18 Atlanta, GA 30339

19 Telephone: (770) 953-0995

20 Fax: (770) 953-1358

21 *Attorneys for Plaintiff Computer Protection IP,*  
22 *LLC*  
23  
24  
25  
26  
27  
28

**Demand for Jury Trial**

Computer Protection hereby demands a trial by jury on all claims and issues so triable pursuant to Fed. R. Civ. Pro. 38(b).

Dated: March 7, 2018

HILL, KERTSCHER & WHARTON, LLP

By: /s/ Vivek Ganti

Vivek Ganti (SBN 275554)

Steven G. Hill (*pro hac vice* pending)

VG@hkw-law.com

SGH@hkw-law.com

HILL, KERTSCHER & WHARTON, LLP

3350 Riverwood Parkway, Suite 800

Atlanta, GA 30339

Telephone: (770) 953-0995

Fax: (770) 953-1358

Scott Vick (SBN 171944)

Scott@vicklawgroup.com

VICK LAW GROUP, APC

800 West Sixth Street, Suite 1220

Los Angeles, California 90017

Telephone: (213) 784-6225

Facsimile: (213) 784-6227

*Attorneys for Plaintiff Computer Protection IP,  
LLC*